



CrimLib.info



Уральский государственный юридический университет
имени В. Ф. Яковлева

АНО "Кримлиб"

Союз криминалистов и криминологов

ТЕХНОЛОГИИ XXI ВЕКА В ЮРИСПРУДЕНЦИИ

4.0

Материалы Четвёртой международной
научно-практической конференции



г. Екатеринбург

20 мая 2022 г.

ФГБОУ ВО
«Уральский государственный юридический университет
имени В. Ф. Яковлева»
АНО «КримЛиб»
Союз криминалистов и криминологов

ТЕХНОЛОГИИ ХХІ ВЕКА В ЮРИСПРУДЕНЦИИ

**Материалы
Четвёртой международной
научно-практической конференции
(Екатеринбург, 20 мая 2022 года)**



Екатеринбург
2022

УДК 34
ББК 67
Т38

Рецензенты:

С. Е. Чаннов, доктор юридических наук, профессор, заведующий кафедрой служебного и трудового права Поволжского института управления имени П.А. Столыпина – филиала федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации»

А. А. Беляков, доктор юридических наук, профессор, заведующий кафедрой криминалистики Уральского государственного юридического университета имени В. Ф. Яковлева

Ответственный редактор:

Д. В. Бахтеев, кандидат юридических наук, доцент, доцент кафедры криминалистики Уральского государственного юридического университета имени В. Ф. Яковлева

Т38 Технологии XXI века в юриспруденции: материалы Четвёртой международной научно-практической конференции (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. — Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева — 2022. — 292 с.

ISBN 978-5-7845-0675-7

В сборнике представлены статьи учёных-юристов, представителей юридической практики и начинающих исследователей, принявших участие в Четвёртой международной научно-практической конференции «Технологии XXI века в юриспруденции», посвящённой отдельным проблемам юридических науки и практики, связанным с современными технологиями.

Мнение авторов может не совпадать с мнением редакции.

УДК 34
ББК 67

ISBN 978-5-7845-0675-7

© Авторы, 2022.
© Уральский государственный
юридический университет имени В. Ф. Яковлева, 2022.

СОДЕРЖАНИЕ

Раздел I

ЦИФРОВЫЕ ТЕХНОЛОГИИ

Кодан Сергей Владимирович

ИНФОРМАЦИОННАЯ КУЛЬТУРА РАБОТЫ С НОСИТЕЛЯМИ
ИНФОРМАЦИИ В НАУЧНОМ ИССЛЕДОВАНИИ 9

Зуев Сергей Васильевич

ОСНОВНЫЕ НАПРАВЛЕНИЯ СБЛИЖЕНИЯ ФИЗИКИ И ПРАВА В
УГОЛОВНОМ ПРОЦЕССЕ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ..... 19

Мазунин Яков Маркиянович, Белова Ксения Сергеевна

ОСОБЕННОСТИ ФИКСАЦИИ ДОПРОСА, ПРОВОДИМОГО С
ИСПОЛЬЗОВАНИЕМ ВИДЕОКОНФЕРЕНЦСВЯЗИ 27

Мещеряков Владимир Алексеевич, Цурлуй Олеся Юрьевна

ДОПРОС В СВЕТЕ ИЗМЕНЕНИЙ, ВНЕСЁННЫХ В УГОЛОВНО-
ПРОЦЕССУАЛЬНОЕ ЗАКОНОДАТЕЛЬСТВО В ДЕКАБРЕ 2021 ГОДА 31

Смахтин Евгений Владимирович

ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ФОРМИРОВАНИЯ ЭЛЕКТРОННЫХ
ДОКАЗАТЕЛЬСТВ И ИХ ПРЕДСТАВЛЕНИЕ В СУД ПЕРВОЙ ИНСТАНЦИИ
..... 39

Бахтеев Дмитрий Валерьевич

ТАКТИКА ИСПОЛЬЗОВАНИЯ ДРОНОВ ПРИ ОСМОТРЕ МЕСТА
ПРОИСШЕСТВИЯ..... 47

Хамидуллин Руслан Сибгатуллович

КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОТИВОДЕЙСТВИЯ
НЕЗАКОННОМУ ОБОРОТУ НАРКОТИЧЕСКИХ СРЕДСТВ И
ПСИХОТРОПНЫХ ВЕЩЕСТВ, ОСУЩЕСТВЛЯЕМОМУ В КРИПТОВАЛЮТЕ
С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ «BLOCKCHAIN» 52

Довгань Ксения Евгеньевна

РАМОЧНОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В
РОССИЙСКОЙ ФЕДЕРАЦИИ 59

Долинин Владимир Николаевич, Пермяков Евгений Константинович, Ровнушкин Вадим Евгеньевич	
ИСПОЛЬЗОВАНИЕ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ	65
Зазулин Анатолий Игоревич	
AUTOMATION BIAS (ОШИБКА АВТОМАТИЗАЦИИ): ЕЩЁ ОДНА ПРОБЛЕМА ВНЕДРЕНИЯ ТЕХНОЛОГИЙ ИИ В ПРАВОСУДИИ.....	76
Карепанов Николай Васильевич	
ОСОБЕННОСТИ ТЕХНОЛОГИИ АГРЕГИРОВАНИЯ, ИССЛЕДОВАНИЯ И ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННО-ЦИФРОВЫХ СЛЕДОВ ПРЕСТУПЛЕНИЯ	86
Нелюбин Константин Александрович	
ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННОЙ БАЗЫ ДАННЫХ ПРИ РАССЛЕДОВАНИИ СЕРИЙНЫХ ПРЕСТУПЛЕНИЙ ПРОТИВ ПОЛОВОЙ СВОБОДЫ И НЕПРИКОСНОВЕННОСТИ	105
Олифиренко Екатерина Павловна	
АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ОРГАНОВ ПРОКУРАТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ	110
Титов Павел Михайлович	
К ВОПРОСУ О НАЧАЛЕ УГОЛОВНОГО ПРЕСЛЕДОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННОЙ СРЕДЫ	116
Шишкина Елена Викторовна	
НЕКОТОРЫЕ АСПЕКТЫ ПРОВЕДЕНИЯ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ С ИСПОЛЬЗОВАНИЕМ ВИДЕОКОНФЕРЕНЦСВЯЗИ	121
Каменев Александр Сергеевич	
АДВОКАТСКИЙ КОНТРОЛЬ В УГОЛОВНОМ ПРОЦЕССЕ: ЭЛЕКТРОННО- ЦИФРОВОЙ АСПЕКТ	129
Медведев Виталий Александрович	
ПРОБЛЕМАТИКА ИНТЕГРАЦИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБРАЗОВАТЕЛЬНЫЙ ПРОЦЕСС ПОДГОТОВКИ КАДРОВ ДЛЯ ОРГАНОВ ВНУТРЕННИХ ДЕЛ	134
Можаева Людмила Евгеньевна, Савченко Дмитрий Геннадьевич	
РЕГУЛИРОВАНИЕ СОЦИАЛЬНЫХ СЕТЕЙ И МЕДИАРЕСУРСОВ КАК ЭЛЕМЕНТ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ	138

Можаева Людмила Евгеньевна, Савченко Дмитрий Геннадьевич	
ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ В ОРГАНАХ, ОБЕСПЕЧИВАЮЩИХ ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ РЕСПУБЛИКИ БЕЛАРУСЬ.....	145
Агеева Анастасия Александровна	
ПРОБЛЕМЫ ПОЛУЧЕНИЯ И ИСПОЛЬЗОВАНИЯ БИОМЕТРИЧЕСКИХ ДАННЫХ ПРЕСТУПНИКОВ-МИГРАНТОВ.....	151
Ржанникова Светлана Сергеевна, Лобанов Руслан Эльмирович	
ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ	157
Садыков Мухтар Бейбутович	
ВНЕДРЕНИЕ АВТОНОМНЫХ СИСТЕМ В ОБЪЕДИНЕННЫХ АРАБСКИХ ЭМИРАТАХ НА ПРИМЕРЕ ПОЛИЦИИ ДУБАЯ: ПРАВОВЫЕ И ТЕХНИЧЕСКИЕ АСПЕКТЫ	162
Льянов Муса Микаилович	
ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ОЦИФРОВКИ, ЦИФРОВИЗАЦИИ И ЦИФРОВОЙ ТРАНСФОРМАЦИИ МАТЕРИАЛЬНЫХ СЛЕДОВ ПРЕСТУПЛЕНИЯ	180
Кириллова Нелли Александровна, Медведев Виталий Александрович	
КИБЕРБУЛЛИНГ КАК ОДИН ИЗ ВИДОВ СОЦИАЛЬНОЙ УГРОЗЫ СЕТИ ИНТЕРНЕТ	187
Рожков Роман Александрович, Медведев Виталий Александрович	
К ВОПРОСУ О СПОСОБАХ ИНТЕРНЕТ-МОШЕННИЧЕСТВА.....	193
Коваленко Наталья Евгеньевна	
ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ПРАВО НА УЧАСТИЕ В ПРАВООТНОШЕНИИ В КАЧЕСТВЕ СУБЪЕКТА	197
Берсенев Евгений Валерьевич	
ОСОБЕННОСТИ ПРОВЕДЕНИЯ ОРМ ПО ВЫЯВЛЕНИЮ НЕЗАКОННЫХ ТРАНЗАКЦИЙ И ДЕЯТЕЛЬНОСТИ, СВЯЗАННЫХ С ЯВЛЕНИЕМ «ВЕБКАМ»	200
Кошетьова Мария Денисовна, Лубянкин Никита Романович	
ЦИФРОВИЗАЦИЯ АДВОКАТУРЫ	206
Пашук Елена Олеговна	

РАЗВИТИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ КАК УГРОЗА КОНФИДЕНЦИАЛЬНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	210
----------------------------------------------------------------------------------------	-----

Рукавишникова Галина Александровна

К ВОПРОСУ ОБ ОБЕСПЕЧЕНИИ КОНСТИТУЦИОННОГО ПРАВА ГРАЖДАН НА ПОЛЬЗОВАНИЕ РОДНЫМ ЯЗЫКОМ В АСПЕКТЕ УГОЛОВНО-ПРОЦЕССУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ.....	217
------------------------------------------------------------------------------------------------------------------------------------------------	-----

Руф Владислав Сергеевич

ПЕРСПЕКТИВА РЕГУЛИРОВАНИЯ NFT.....	222
------------------------------------	-----

Сарксян Зоя Феликсовна

ГРАЖДАНСКО-ПРАВОВАЯ ОТВЕТСТВЕННОСТЬ ЗА ДЕЙСТВИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД.....	227
-------------------------------------------------------------------------------------------------------------------	-----

Соколова Анастасия Юрьевна

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОХРАНЫ ПРАВ СОБСТВЕННОСТИ НА РЕЗУЛЬТАТЫ ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ	235
-------------------------------------------------------------------------------------------------------	-----

Цветкова Анна Денисовна

ПРАВОВЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ КЕЙЛОГГЕРОВ.....	240
----------------------------------------------	-----

Эмирбеков Фарид Язиекович

ВОЗМОЖНОСТЬ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ СЛЕДОВАТЕЛЯ.....	248
---------------------------------------------------------------------------------------------------------	-----

Раздел II

БИОТЕХНОЛОГИИ

Рачева Нелли Витальевна, Костин Никита Олегович

ДНК-ФЕНОТИПИРОВАНИЕ И КРИМИНАЛИСТИКА: ПЕРСПЕКТИВЫ СОТРУДНИЧЕСТВА.....	256
--------------------------------------------------------------------------	-----

Рачева Нелли Витальевна, Слепухина Яна Михайловна

ВИРТУАЛЬНОЕ ВСКРЫТИЕ: ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ	266
------------------------------------------------------------------------------	-----

Юдин Егор Витальевич

ПРАВО ПАЦИЕНТА НА ПОЛУЧЕНИЕ ИНФОРМАЦИИ О СОСТОЯНИИ ЗДОРОВЬЯ ПРИ ИСПОЛЬЗОВАНИИ МЕДИЦИНСКИХ ГЕНЕТИЧЕСКИХ	
-----------------------------------------------------------------------------------------------------------	--

ТЕХНОЛОГИЙ: ПЕРЕОСМЫСЛЕНИЕ СУЩЕСТВУЮЩЕГО ПРАВОВОГО МЕХАНИЗМА	274
--------------------------------------------------------------------	-----

Артамонова Дарья Алексеевна

ПРАВОВАЯ ПРИРОДА ДОГОВОРА СУРРОГАТНОГО МАТЕРИНСТВА ...	280
--------------------------------------------------------	-----

Кушнарёв Александр Сергеевич

О НЕКОТОРЫХ ПРОБЛЕМАХ ПРАВОВОГО РЕГУЛИРОВАНИЯ ТЕХНОЛОГИИ МНОГОМЕРНОЙ БИОПЕЧАТИ.....	287
-------------------------------------------------------------------------------------	-----

Раздел I

ЦИФРОВЫЕ ТЕХНОЛОГИИ

Блокчейн, NFT и технологии распределённого реестра

Искусственный интеллект и машинное обучение

Интернет, социальные сети и медиаресурсы

Электронные (цифровые) доказательства

Использование компьютерных технологий в правоохранительной деятельности

Электронное правосудие, электронный документооборот

Общие вопросы регулирования цифровых технологий

УДК 340.130.4

Кодан Сергей Владимирович

Доктор юридических наук, профессор,
Заслуженный юрист Российской Федерации,
главный научный сотрудник Управления научных исследований,
профессор кафедры теории государства и права,
Уральский государственный юридический университет им. В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
svk2005@yandex.ru

ИНФОРМАЦИОННАЯ КУЛЬТУРА РАБОТЫ С НОСИТЕЛЯМИ ИНФОРМАЦИИ В НАУЧНОМ ИССЛЕДОВАНИИ*

Аннотация: В статье основное внимание акцентируется на проблеме взаимодействия научной и информационной культур в исследовательских практиках как взаимосвязанных явлений в условиях развития современного информационного общества. Особое внимание обращается на проявления недобросовестной работы с носителями информации и информационных возможностях их выявления.

Ключевые слова: научная культура, информационная культура, научно-информационные ресурсы, понятийное мышление, концептуальное мышление, клиповое мышление, девиантные проявления в науке, некорректное заимствование, рерайтинг, копи-паст.

Для цитирования:

Кодан С. В. Информационная культура работы с носителями информации в научном исследовании // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 9–18.

Развитие информационного общества существенно расширяет возможности доступа к информационным ресурсам, делает их более доступными и позволяет исследователю оперативно получать сведения, необходимые для научной работы. Современные информационные технологии, которые стали неотъемлемым атрибутом

научно-исследовательских практик, одновременно становятся и предметом повышенного внимания к их использованию в контексте научной культуры в целом. Эта проблема является особенно актуальной в социогуманитаристике в плане и связана с получением достоверных, доказанных и проверяемых знаний, основанных на тщательно отобранных

* Публикация подготовлена в рамках реализации финансируемого РФФИ научного проекта 20-011-00779 «Историография, источниковедение и методология истории политических и правовых учений: теоретические и прикладные проблемы исследовательских практик».

и критически оценённых исследователями носителях социальной информации. Остановлюсь на основных проблемных пространствах взаимодействия научной культуры и культуры информационной.

1. Взаимосвязь научной культуры и информационной культуры в научной деятельности очевидны. В этих обстоятельствах самые общие требования научной культуры к учёному – интеллектуальная честность, интеллектуальная добросовестность, исследовательская компетентность – в преломлении к информационной культуре определяют её базисные основания по отношению к работе исследователя с информационными ресурсами. Это связано с тем, что в современном научном и образовательном пространстве через посредство информационных ресурсов в научной культуре, как подчёркивает М. К. Мамардашвили, «выражена и репродуцируется способность человека владеть им же достигнутым знанием универсума и источниками этого знания и воспроизводить их во времени и пространстве»¹. Эти способности учёного в современном информационном обществе, находящемся в стадии движения к обществу знаний, требуют обеспечить «возможность находить, производить, обрабатывать, преобразовывать, распространять и использовать

информацию с целью получения и применения необходимых для человеческого развития знаний»². Одновременно следует учитывать и то, что именно анализ оригинальности и научной новизны научного исследования требует соблюдения правила, которое весьма чётко определил А. И. Ракитов и которое состоит в том, что «та или иная единица научного знания считается новой, если она отвечает требованиям научности и к моменту ее создания отсутствует в списке ранее установленных научных знаний» и тем самым выступает как «критерий новизны»³.

Информационная культура исследователя носит личностный характер и, как определяет С. Д. Каракозов, «представляет собой составную часть базисной культуры личности как системной характеристики человека, позволяющая ему эффективно участвовать во всех видах работы с информацией: получении, накоплении, кодировании и переработке любого рода, в создании на этой основе качественно новой информации, ее передаче, практическом использовании и включающая грамотность и компетентность в понимании природы информационных процессов и отношений, гуманистически ориентированную информационную ценностно-смысловую сферу (стремления,

¹ Мамардашвили М. К. Наука и культура // Методологические проблемы историко-научных исследований. М., 1982. С. 42.

² К обществам знания. Всемирный доклад ЮНЕСКО. Париж, 2005. С. 7.

³ Ракитов А. И. Философские проблемы науки. Системный подход. М., 1977. С. 149–150.

интересы, мировоззрение, ценностные ориентации), развитую информационную рефлексию, а также творчество в информационном поведении и социально-информационной активности»⁴. Указанное определение и заложенные в нём характеристики информационной культуры личности относительно её научно-культурных аспектов требуют определённых корректив, поскольку проблема все больше уходит не только и не столько исключительно к личным знаниям и навыкам работы с информационными ресурсами (собственно в данное явление), а становится одной из проблем научной культуры в целом. На первый план, как мне представляется, выдвигаются вопросы выработки научным сообществом конвенциональных норм и правил этического, методологического и технологического характера, позволяющих снизить риски проявлений недобросовестности в использовании информационных ресурсов. Развитие аппаратного и программного потенциала для работы с источниками социальной информации в научно-исследовательских практиках безусловно способствуют преодолению рутинности определённых их этапов, позволяют меньше тратить усилий на поиск и обработку источников познания социальных институтов и, в конечном итоге, повышают результативность усилий учёного.

⁴ Каракозов С. Д. Информационная культура в контексте общей культуры личности // Педагогическая информатика. 2000. № 2. С. 55.

Информационные ресурсы и технологии в современной научно-познавательной деятельности учёного стали качественно новым исследовательским инструментом в работе с носителями социальной информации, посредством которых исследователь получает широкие возможности для оперативного и многоаспектного доступа к различным источникам социальной информации на основе современных информационных баз данных и технологий обработки различного рода информации. Неоспоримым стал отмечаемый в науковедении факт того, что «даже в рамках традиционно организованной научной деятельности пользователи интернет-технологий получили безусловное преимущество перед коллегами, не использующими компьютерные телекоммуникации», – справедливо подчёркивает Е. З. Мирская⁵. При этом информационные ресурсы и исследователь в научно-познавательной деятельности в условиях современного информационного общества условиях тесно взаимосвязаны.

Научная деятельность учёного опирается на информационное мировоззрение и его включённость в информационное пространство, связанные потребностями в получении информации. Из этого следует запрос исследователя на необходимость информационного обеспечения работы с носителями информации и получение достоверных эмпирических данных

⁵ См.: Мирская Е. З. Наука в информационном обществе: новые возможности и проблемы // Информационное общество. 2005. № 5. С. 4–7.

для научной работы. В указанных планах доступность, достоверность и надёжность информационных ресурсов при надлежащем использовании представляемых через их посредство носителей информации выступают одной из важнейших, а информационные ресурсы позволяют обеспечить контроль за качеством исследовательского материала. Но при этом появляются и «соблазны» быстрого и поверхностного получения «результата», который нередко не соответствует критериям получения нового знания как знания достоверного и проверяемого. Именно поэтому и представляется важным обратиться к отдельным проблемным полям, взаимосвязанным и находящимся на пересечении научной и информационной культур, на которых и остановлюсь далее.

2. Клиповое мышление как проблема в информационной и научной культуре находится в плоскости рассмотрения проблематики его соотношения с понятийным мышлением и непосредственно связано с научно-исследовательскими практиками. Эти уровни мышления в современных условиях в их взаимодействии выступают системообразующими как в сочетании традиционных и новых форм восприятия информации, так определяют качество её обработки исследователем. При этом указанные типы мышления в большинстве имеющихся исследований преимущественно не только

противопоставляются, но и (чаще всего) подчёркивается крайне негативное отношение к клиповому мышлению и даже апокалиптически утверждается, что оно «приводит к интеллектуальной деградации, представляя собой угрозу для общества»⁶. При этом особо отметим, что проблема соотношение клипового и понятийного мышления не должна рассматриваться в «чёрно-белом» варианте и требует выработки методологических подходов относительно включенности клипового мышления в процессы понятийного осмысления информации.

Клиповое мышление исходит из понимания термина «клип», который происходит от англоязычного обозначения им «вырезки из газеты» и означает своего рода «вырезку» из потока информации в мыслительной деятельности человека. Этот тип мышления, по утверждению ряда исследователей, имеет следующие основные негативные черты: низкая концентрация на содержании информации, поверхностное её восприятие и усвоение; неспособность к глубокому критическому анализу и синтезу полученной информации и принятию взвешенных выводов и решений; подверженность носителей этого типа мышления внешнему манипулированию и др. В итоге «клиповое мышление мешает аналитическим способностям, поскольку образы, которые остаются в мыслях только на короткий промежуток времени, практически

⁶ Крайнов А. Л. Клиповое мышление в контексте образовательных практик: социально-философский анализ // Известия

Саратовского университета. Новая серия. Серия: Философия. Психология. Педагогика. 2019. Т. 19, № 3. С. 262.

сразу исчезают и заменяются новыми». И, напротив, *понятийное мышление*, которое является системным и направлено на более длительное по времени, но более глубокое и критическое осмысление информации с анализом и синтезом её содержания, выделением существенных признаков представленной в ней сведений о социальных явлениях, процессах, институтах и т. п. Соответствующее этим видам мышления деление людей включает два их типа – «люди книги» и люди экрана». Первые из указанных типов – это «люди, читающие книги, а под книгами мы подразумеваем как бумажные, так и электронные книги, любой текст достаточно большого объёма, имеющий линейную структуру, обладают понятийным мышлением, способны углубляться в информацию, находить и выделять существенные признаки в изучаемой предметной области, анализировать полученную информацию и делать выводы, используя способность к критическому мышлению». Второй тип – это «новое поколение, так называемые «люди экрана», обладают визуальным, быстрым, но поверхностным мышлением, получившим название «клиповое мышление». Им присущ языковой минимализм и речевая бедность, рассеянность и гиперактивность, дефицит внимания. У них конкретное мышление преобладает над абстрактным», – отмечают М. А. Купчинская и Н. В. Юдалевич⁷.

⁷ См.: Купчинская М. А., Юдалевич Н. В. Клиповое мышление как феномен современного общества // Бизнес-образование в экономике знаний. 2019. № 3. С. 66–70.

Характерно, что указанные оценки дают лишь общее представление об указанных явлениях, но не определяют конструктивных подходов к их взаимодействию в современном информационном обществе.

Одновременно необходимо учитывать и то, что в практиках научных исследований большое значение имеет и *латеральное мышление*, которое выступает как мышление креативное и под которым понимается процесс обработки информации на основе активного использования творческих способностей и интуиции, быстроты и гибкости ума, способности к продуцированию новых идей и прогностичности – предвидения новых научных результатов. Этот тип мышления отличается от традиционного, логического мышления с его последовательной пошаговой обработкой информации и внешне логической взаимосвязанной и взаимообусловленной цепочкой оправданных решений для достижения результата⁸.

При этом ряд авторов справедливо акцентирует внимание именно на позитивных свойствах клипового мышления, которые состоят в том, что оно в сложном информационном пространстве значительно ускоряет познавательную деятельность и акцентирует внимание на наиболее важной информации в режиме данного момента её восприятия во времени, способность к

⁸ См.: Милёхина О. В., Захарова Е. Я. Латеральное мышление как фактор обеспечения успешности работы // Вестник Томского государственного университета. Экономика. 2012. № 4. С. 28–35.

работе условиях многозадачности, избытка информационных ресурсов и дефицита времени для их обработки⁹. Соответственно возникает и вопрос о возможности включения клипового мышления в научно-познавательные процессы и моделях его использования в исследовательских практиках.

Представляется, что «клип» в научно-познавательной деятельности выступает в качестве поискового инструмента и посредством «опознавательного образа» – восприятия целого в основе которого находится до минимума «сокращённое понятие» – позволяет быстро сориентироваться в больших объёмах информации и обеспечить поиск именно необходимой информации с последующим её понятийным осмыслением и использованием возможностей латерального мышления. «Клиповый характер поступления информации, безусловно, требует нового характера ее обработки и порождает новый тип мышления – концептуальное, поскольку очевидно, что функции анализа и синтеза не исчезают, а переключаются на новый, более высокий уровень обобщения информации и выявления смыслов, а сознание, развивающееся в контексте клиповой информационной среды, не может не продуцировать эвристических решений тех или иных задач как в повседневной деятельности, так и в

профессиональной», – справедливо обращает внимание на необходимость учёта особенности обработки информации при клиповом мышлении И. Г. Пендикова¹⁰. Именно такой подход к использованию клипового мышления – объяснение его позитивных сторон и возможностей использования в процессе исследовательских практик – необходимо прорабатывать в процессе подготовки молодых исследователей. Именно тогда клиповый тип мышления вполне может способствовать более быстрой адаптации исследователя в потоках и огромном массиве информации, которая должна находиться в поле его зрения в рамках научной работы.

3. Выявление и предупреждение проявлений ненадлежащего использования информационных ресурсов связаны с нарушением как требований к общей научной культуре, так и к культуре информационной. На их пересечении возникает весьма актуальная проблема изучения *информационных рисков в научно-исследовательских практиках*, которые могут рассматриваться как возможность непреднамеренного или преднамеренного включения автором в научную работу недостоверных или искажённых данных как следствия ненадлежащего подбора, анализа и репрезентации в исследовании носителей информации, на которых

⁹ См.: Семеновских Т. В. «Клиповое мышление» – феномен современности // Оптимальные коммуникации (ОК). Эпистемический ресурс Академии медиаиндустрии и кафедры теории и практики общественной связности РГГУ.

URL: <http://jarki.ru/wpress/2013/02/18/3208/> (дата обращения: 12.05.2022).

¹⁰ Пендикова И. Г. Клиповое и концептуальное мышление как разные уровни процесса мышления // Омский научный вестник. Серия: Общество. История. Современность. 2016. № 1. С. 54.

основаны положения научной работы. В конечном итоге это влияет на качество научных работ различного уровня – от тезисов выступлений на конференциях до диссертационных исследований – и вызывает серьёзную обеспокоенность научного сообщества. При этом особо подчеркнём, что именно современные информационные возможности – соответствующее программное обеспечение и методики его использования – позволяют не только их своевременно выявить, но и выступают важным средством предупреждения проявлений недобросовестного поведения в науке.

Формы проявления ненадлежащего использования информационных ресурсов прежде всего связаны с использованием средств некорректного заимствования тестов предшествующих исследований и создания на их основе «новых научных текстов». По существу, все это, как подчёркивает академик Д. С. Лихачев, «воровство в науке – пользоваться чужими материалами, не ссылаясь на истинных их владельцев»¹¹.

Выделим основные конфигурации указанного поведения в исследованиях.

Плагиат – публикация под своим именем чужого произведения или его фрагментов без принятого в науке обозначения цитирования – ссылки на оригинальный (исходный)

источник – публикацию. Выделяются основные формы плагиата: *прямой* – непосредственное заимствование «слово в слово» без указания источника и *мозаичный* – переплетение собственного текста с включением незначительных заимствований из чужих тестов без указания источников¹².

Рерайтинг – присвоение чужих идей, концепций, методов посредством переработки исходных текстов, изложения их в другой текстуальной редакции без ссылок на источники заимствованных научных положений. В данном случае авторский текст (или тексты) непосредственно не заимствуется и за свои собственные идеи выдаются заимствованные и основательно перефразированные подходы других авторов, т. е. происходит «переписывание текста с изменением формы изложения и сохранением смысла оригинала»¹³. При этом рерайтинг производится «путём замены слов их синонимами; посредством перевода прямой речи в косвенную; изменением последовательности изложения основных фрагментов текста, а также грамматического строя самих предложений; путём исключения из текста фрагментов, не несущих смысловой нагрузки, либо добавления таковых; увеличением количества причастных и деепричастных оборотов; переписыванием текста по памяти после прочтения и др.»¹⁴.

¹¹ Лихачев Д. С. Прошлое – будущему. Статьи и очерки. Л., 1985. С. 569.

¹² См.: Островская А. С. Плагиат в XXI веке: кому это нужно? // Вопросы современной педиатрии. 2016. Т. 15, № 2. С. 148–150.

¹³ Белькова Е. Г. Рерайтинг: правовая оценка // Проблемы современного российского законодательства. Иркутск, 2013. С. 142.

¹⁴ Еремченко В. И., Щуров Е. А. Рерайтинг: механизм преступной деятельности и проблемные вопросы расследования //

Копи-паст – составление компилятивного авторского текста из незначительных фрагментов чужих текстов с различных сайтов без указания ссылок на авторство и источник информации и представление для публикации или размещения на web-ресурсе. Такие статьи-компиляции имитируют научную работу и отличаются большим количеством размытых формулировок и выводов, которые часто не несут никакой смысловой нагрузки. Они также характеризуются отсутствием логически выверенным построением и не представляют собой целостный, завершённый текст в рамках предмета исследования. Сюда же примыкают и так называемые «мигрирующие цитаты», к которым, как правило, относятся термины и определения и ссылки на которые отсутствуют. Нередко такие цитаты, вырванные из концепции и контекста, в совокупности с отсутствием ссылки на исходный текст, порождают проблемы оценки достоверности, точности и доказанности нового знания, претендующего на новое, а также создаётся видимость знания как «аксиоматического»¹⁵.

Признание наличия плагиата, рерайтинга и копи-паста должно проводиться на основе экспертизы двух (или более) текстов как носителей информации на предмет совпадения

представленных в них текстов. Выявление и оценка таких фактов не должна сводиться исключительно к технической стороне проверки работы в системах автоматизированной проверки, возможности которых представляют отечественные программы «Антиплагиат», «Advego Plaguatus», «eTXT Антиплагиат» и др. Указанные программные средства дают лишь исходный материал для аналитической работы на предмет выявления указанных проявлений недобросовестности и их результаты выступают в качестве основы для принятия решения о признании таковым текста, совпадающего со сравниваемым предшествующим текстом.

Итак, обозначенные контуры основных проблем взаимодействия и взаимовлияния научной культуры и культуры информационной показывают как их значение в обеспечении качественной информационной базы научного исследования, так и необходимость изучения этой проблематики. В условиях развития современного информационного общества качественное использование информационных ресурсов обеспечивает и качество исследовательских практик, и получаемого в их ходе результатов научной деятельности.

Вестник Казанского юридического института МВД России. 2018. № 3. С. 367.

¹⁵ См.: Игнатович Е. В. Явление копи-паст в сфере научных публикаций о непрерывном образовании // Непрерывное образование: XXI век. 2017. № 3. С. 98–114; Барчунова Т.

В. Эссе о копипасте: заимствование, компиляция, плагиат // Вестник Новосибирского государственного университета. Серия: Философия. 2014. Т. 12, № 2. С. 58–66.

Список литературы

1. Барчунова Т. В. Эссе о копипасте: заимствование, компиляция, плагиат // Вестник Новосибирского государственного университета. Серия: Философия. 2014. Т. 12, № 2. С. 58–66.
2. Белькова Е. Г. Ререйтинг: правовая оценка // Проблемы современного российского законодательства. Иркутск, 2013. С. 142–146.
3. Еремченко В. И. Ререйтинг: механизм преступной деятельности и проблемные вопросы расследования / В. И. Еремченко, Е. А. Щуров // Вестник Казанского юридического института МВД России. 2018. № 3. С. 365–369.
4. Игнатович Е. В. Явление копи-паст в сфере научных публикаций о непрерывном образовании // Непрерывное образование: XXI век. 2017. № 3. С. 98–114.
5. К обществам знания. Всемирный доклад ЮНЕСКО. Париж, 2005. 231 с.
6. Каракозов С. Д. Информационная культура в контексте общей культуры личности // Педагогическая информатика. 2000. № 2. С. 55. С. 41–55.
7. Крайнов А. Л. Клиповое мышление в контексте образовательных практик: социально-философский анализ // Известия Саратовского университета. Новая серия. Серия: Философия. Психология. Педагогика. 2019. Т. 19, № 3. С. 262–266.
8. Купчинская М. А. Клиповое мышление как феномен современного общества / М. А. Купчинская, Н. В. Юдалевич // Бизнес-образование в экономике знаний. 2019. № 3. С. 66–70.
9. Лихачев Д. С. Прошлое – будущему. Статьи и очерки. Л., 1985. 575 с.
10. Мамардашвили М. К. Наука и культура // Методологические проблемы историко-научных исследований. М., 1982. С. 38–58.
11. Милёхина О. В. Латеральное мышление как фактор обеспечения успешности работы / О. В. Милёхина, Е. Я. Захарова // Вестник Томского государственного университета. Экономика. 2012. № 4. С. 28–35.
12. Мирская Е. З. Наука в информационном обществе: новые возможности и проблемы // Информационное общество. 2005. № 5. С. 4–7.
13. Островская А. С. Плагиат в XXI веке: кому это нужно? // Вопросы современной педиатрии. 2016. Т. 15, № 2. С. 148–153.
14. Пендикова И. Г. Клиповое и концептуальное мышление как разные уровни процесса мышления // Омский научный вестник. Серия: Общество. История Современность. 2016. № 1. С. 53–56.
15. Ракитов А. И. Философские проблемы науки. Системный подход. М., 1977. 270 с.
16. Семеновских Т. В. «Клиповое мышление» – феномен современности // Оптимальные коммуникации (ОК). Эпистемический ресурс Академии медиаиндустрии и кафедры теории и практики общественной связности РГГУ. URL: <http://jarki.ru/wpress/2013/02/18/3208/>.

Sergey V. Kodan

Doctor of Law, Professor, Honored Lawyer of the Russian Federation,
Chief Researcher of the Department of Scientific Research,
Professor of the Department of Theory of State and Law,
Ural State Law University named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
svk2005@yandex.ru

**INFORMATION CULTURE OF WORKING WITH MEDIA IN SCIENTIFIC
RESEARCH**

Abstract: The article focuses on the problem of the interaction of scientific and information cultures in research practices as interrelated phenomena in the conditions of the development of modern information society. Particular attention is paid to the manifestations of unfair work with information carriers and the information possibilities of their detection.

Keywords: scientific culture, information culture, scientific and information resources, conceptual thinking, conceptual thinking, clip thinking, deviant manifestations in science, incorrect borrowing, rewriting, copy paste.

УДК 343.131

Зуев Сергей Васильевич

Доктор юридических наук, доцент,
профессор кафедры правоохранительной деятельности
и национальной безопасности,
Южно-Уральский государственный университет
(г. Челябинск, Российская Федерация)
zuevsergej@inbox.ru

ОСНОВНЫЕ НАПРАВЛЕНИЯ СБЛИЖЕНИЯ ФИЗИКИ И ПРАВА В УГОЛОВНОМ ПРОЦЕССЕ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация: В статье автор утверждает, что цифровизация приводит к сближению точных и гуманитарных наук, в частности физики и права в уголовном процессе. Определяет основные направления данного явления, которые связаны с развитием информационных отношений в уголовном судопроизводстве, широким применением электронно-технических средств в доказывании по уголовным делам, а также с взаимодействием материальных уголовно-процессуальных объектов.

Ключевые слова: цифровизация, уголовный процесс, физика, право, электронная информация.

Для цитирования:

Зуев С. В. Основные направления сближения физики и права в уголовном процессе в условиях цифровизации // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 19–26.

Физика и право в уголовном процессе, на первый взгляд, две вещи несовместимые. И вместе с тем, следует констатировать не только наличие этих двух феноменов, но и их сближение в условиях цифровизации. И здесь необходимо отметить некоторые важные аспекты. Прежде всего, следует выделить отдельные направления формирования научных знаний, в которых наблюдается такое явление.

Первое. По линии развития информационных отношений в уголовном судопроизводстве.

Информация становится центральным объектом исследований в сфере как точных наук, так и гуманитарных, право не является исключением. Информацию пытаются определить как категорию, измерить, успешно передавать, сохранять, копировать.

Начало изучению категории «информация» положено в 20-х годах XX столетия. При этом количественная характеристика легла в основу понимания сущности данного явления. Информацию стали понимать, к примеру, как:

– меру снятой неопределенности¹;

– изменение содержащейся в системе собственной смысловой информации за счёт накопления информации внешней²;

– изменение запаса знаний (тезауруса)³;

– отражённое различие⁴;

– маркированное детерминированным способом конечное множество физически измеримых параметров изделия-носителя⁵.

Несмотря на различия в определении сущности изучаемого феномена, объединяющими элементами в данном случае могут выступить такие понятия, как «сигнал» и «смысл». Сигнал имеет материальную, а значит физическую составляющую. Тогда как смысл необходим, чтобы можно было отличить набор случайных символов от связанных между собой знаков, что и позволит судить об изменениях в сознании, событиях, действиях.

Объединяющим также выглядит подход в представлении информации как одного из «свойств реальности, которое проявляется в неоднородности (асимметрии) распределения материи и энергии в пространстве и в неравномерности протекания во времени всех процессов, происходящих в мире живой и неживой природы, а также в человеческом обществе и сознании»⁶.

Информационные отношения в уголовном судопроизводстве занимают важное место, так как позволяют получать доказательства, содержанием которых становится информация⁷. Кроме того, ориентирующая информация способствует выдвижению версий, определению направления расследования, даёт представление о полной картине изучаемого события⁸.

Второе. *В области широкого применения электронно-технических средств в доказывании по уголовным делам.*

Физику и право в уголовном процессе на современном этапе

¹ См.: Шенон К. Работы по теории информации и кибернетике. М, 1963. С. 10.

² Шрейдер Ю. А. Об одной модели семантической теории информации // Проблемы кибернетики. 1965. Вып. 3. С. 233–240.

³ Шрейдер Ю. А. Тезаурусы в информатике и логической семантике // Научно-техническая информация. 1971. Сер. 2, № 3. С. 9.

⁴ Хохлов Г. И. Основы теории информации: учеб. пособие. М., 2008. С. 84.

⁵ Гадасин В. А. Концепция триад – понятие «информация» как субстанция // Ежегодник ВНИИ-ПВТИ: Сб. науч. тр. Минск, 2007. С. 191.

⁶ Колин К. К. Философия информации: структура реальности и феномен

информации // Метафизика. 2013. № 4 (10). С. 73.

⁷ Тушев А. А., Назаров Н. А. Информация как основа всех видов доказательств в уголовном процессе // Общество и право. 2012. № 3 (40). С. 195–197; Яковлева О. А. Классификация криминалистически значимой информации и ее роль в досудебном уголовном производстве // Вестник Волгоградского государственного университета. Серия 5: Юриспруденция. 2016. Т. 15, № 1 (30). С. 189–193.

⁸ См.: Корма В. Д. Информационный аспект следственной деятельности // Вестник университета имени О. Е. Кутафина (МГЮА). 2021. № 2 (78). С. 27–36.

объединяет обращение участников уголовного судопроизводства с электронной информацией. Это и её копирование, и изъятие вместе с материальными носителями. Вокруг этого проведено много исследований⁹.

Интерес к электронной информации возник в связи с широким использованием доказательств в электронном виде, что породило много вопросов, связанных с достоверностью полученной информации. Особое внимание заслуживают виды электронных носителей информации, поскольку с ними закон связал обязательное участие специалиста (ст. 164.1 УПК РФ).

Электронная информация легко может быть подвергнута модификации. При этом порой очень сложно определить следы, указывающие на внесение изменений.

Особенностью сигнала, передаваемого посредством электронно-технических устройств, является его дискретная форма, которая имеет знаковое и цифровое обозначение. В электронных системах за счёт специальных программ, использующих определённые алгоритмы, происходит кодирование и декодирование сигналов. Это, прежде всего, относится к цифровой

электронной информации. Аналоговая информация через преобразователь также может стать цифровой.

Согласно ГОСТ 2.051-2013 «Единая система конструкторской документации. Электронные документы.» под электронным носителем информации следует понимать «материальный носитель, используемый при записи, хранении и воспроизведении информации, обрабатываемой с помощью средств вычислительной техники».

Важное свойство электронного носителя информации – пригодность для хранения информации. На его наличие указывают и другие авторы. Так, например, О. Г. Григорьев пишет о том, что носители компьютерной информации отличаются техническими устройствами записи, хранения и воспроизведения информации¹⁰. Ю. В. Гаврилин также подчеркивает, что электронный носитель информации – это устройство, конструктивно предназначенное для постоянного или временного хранения информации в виде, пригодном для использования в электронных вычислительных машинах»¹¹.

Споры о том, что является электронным носителем информации,

⁹ См., например: Овсянников Д. В. Доказательственное значение результатов копирования электронной информации в уголовном процессе // Правопорядок: история, теория, практика. 2015. № 2 (5). С. 3–36; Маслов А. В., Соскова К. А. Электронная информация, как доказательство по уголовным делам // Центральный научный вестник. 2017. Т. 2, № 11 (28). С. 57–59; Ларин Е. Г. Копирование информации с электронных носителей при производстве по уголовному делу //

Законодательство и практика. 2012. № 2 (29). С. 52–53.

¹⁰ Григорьев О. Г. Роль и уголовно-процессуальное значение компьютерной информации на досудебных стадиях уголовного судопроизводства: дис. ... канд. юрид. наук. Тюмень, 2003. С. 58.

¹¹ Гаврилин Ю. В. Электронные носители информации в уголовном судопроизводстве // Труды академии управления МВД России. 2017. № 4 (44). С. 47.

продолжаются. И здесь без учёта их физических особенностей юристам не решить вопрос о правомерности тех или иных процессуальных действий, связанных с изъятием таких материальных носителей.

Третье. *При взаимодействии материальных объектов в сфере уголовного судопроизводства.*

Уголовно-процессуальные отношения являются разновидностью правовых, и далее, социальных отношений, обязательным элементом которых выступает человек. В правовых отношениях принято выделять субъектов, наделённых совокупностью прав и обязанностей.

Одновременно, человек может рассматриваться как часть материального, а значит физического мира. Это предполагает наличие у него соответствующих свойств. Кроме того, в уголовно-процессуальных отношениях могут фигурировать предметы, вещества, живые организмы. В каком-то смысле о них можно говорить как об объектах.

Объекты окружающего мира – это любые предметы, явления, процессы, которые могут восприниматься человеком как целое.

Каждый объект наделён именем, имеет свойства и параметры, характеризуется действиями и состоянием. Свойства и параметры имеют физическую природу, не учитывать которую невозможно. Зная параметры, их пределы можно оценивать степень возможного осуществления чего-либо, а значит,

пределы допустимого. Последнее может включать в себя допустимость доказательств, но не исчерпываться этим.

К свойствам уголовно-процессуальных объектов можно отнести, например, размер, массу, твёрдость, плотность, упругость, особенности функционирования, различные способности (изменять агрегатное состояние, отражать определённый спектр цвета, сохранять во времени свои существенные признаки, изменять объём в зависимости от изменения температуры, адсорбировать¹², смешиваться с другими жидкостями или растворяться в них, если речь идёт о твёрдых телах, и др.).

Объекты, в том числе уголовно-процессуальные, могут выполнять действия как самостоятельно, так и под влиянием других объектов, меняя при этом своё состояние. Последовательную смену состояний называют процессом. Мы под этим будем иметь в виду не просто смену стадий уголовного судопроизводства, а именно то, что указывает на смену состояний объекта (объектов). Состояние может иметь информационную составляющую, и тогда следует выделять информационные процессы, включающие сбор, хранение, обработку, передачу информации.

Наличие самого объекта может иметь процессуальное значение. Так, например, невозможность физического присутствия лица в зале

¹² Адсорбция – поглощение вещества из раствора или газа поверхностным слоем жидкости или твердого тела.

суда лежит в основе применения видеоконференцсвязи.

Особое внимание здесь необходимо обратить на способность предметов к отражению. Д. И. Бедняков отмечает, что процессы отражения существуют на всех ступенях развития материального мира¹³.

В неживой природе результатом взаимодействия являются следы (изменения, отпечатки), понимаемые как углубление, знак, метка от надавливания, прикосновения, царапания, сохранившаяся, уцелевшая часть, остаток чего-нибудь, изменение физического, химического либо биологического строения и состава вещества.

Несколько иначе процесс отражения происходит в живой природе. Так, простейшие живые организмы не обладают способностью к отражению, они отличаются лишь раздражимостью¹⁴. Человек обладает сознанием. Процесс отражения у него происходит идеально (на уровне сознания) с помощью речи и языка и характеризуется активностью познающего субъекта, включением результатов отражения в дальнейшую деятельность.

Предметы материального мира существуют объективно, то есть независимо от нашего сознания. Чтобы получить какие-либо знания о предмете, человек должен воспринять его с помощью своих органов чувств, переработать в сознании и

сформировать образно-знаковую информационную модель данного предмета. Только после этого предмет получит субъективное выражение в форме знаний человека, сведений, информации. Иными словами, человек является производителем информации и без него невозможно её возникновение. Такая мысль поддерживается профессором М. П. Поляковым¹⁵.

Среда влияет на объект. Любое взаимодействие объектов между собой и со средой предполагает отражение и оставляет следы: материальные (на любых объектах), идеальные (в сознании), цифровые (на электронных носителях информации).

Цифровые следы представляют собой «результат действий человека или автоматизированной системы, воплощённые, как правило, в текстовой или мультимедийной форме и пригодные к трансформации в доказательства по уголовным делам. Например, констатируется, что при расследовании получения взятки следователем часто фиксировались электронные следы, указывающие на подготовительные действия преступника (предварительная договорённость о встречах взяткодателя с взяткополучателем, согласие на участие в качестве посредника при передаче-получении взятки), так как преступное общение между взяткодателем и взяткополучателем было не при личном контакте, а при использовании

¹³ Бедняков Д. И. Непроцессуальная информация и расследование преступлений. М., 1991. С. 24.

¹⁴ Введение в психологию: учебное пособие / под ред. А. В. Петровского. М., 1995. С. 367.

¹⁵ Поляков М. П. Уголовно-процессуальная интерпретация результатов оперативно-розыскной деятельности: монография. Н. Новгород, 2001. С. 149.

средств компьютерной техники, мобильных устройств, когда информационный обмен осуществлялся с помощью SMS-сообщений, сообщений в мессенджерах, электронных писем и фиксация факта передачи-получения взятки также была на электронных информационных носителях»¹⁶.

Уголовно-процессуальные объекты могут быть представлены как физические тела, подчиняющиеся законам механики, электродинамики и других выделяемых разделов физики как науки. Объекты имеют протяжённость, занимают определённое место в пространстве, располагаются конкретным

воспринимаемым образом, могут быть задействованы для осуществления уголовного судопроизводства.

Таким образом, в трёх обозначенных направлениях можно наблюдать сближение таких наук, как физика и право. Понимание этого может дать дополнительный импульс развитию уголовно-процессуальных отношений, их правовому регулированию. Дополнительным толчком может послужить использование искусственного интеллекта для решения задач уголовного судопроизводства и переход на производство по уголовным делам в электронном виде.

Список литературы

1. Бедняков Д. И. Непроцессуальная информация и расследование преступлений. М.: Юридическая литература, 1991. 208 с.
2. Введение в психологию: учебное пособие / под ред. А. В. Петровского. М.: МГУ, 1995. 546 с.
3. Гаврилин Ю. В. Электронные носители информации в уголовном судопроизводстве // Труды академии управления МВД России. 2017. № 4 (44). С. 45–50.
4. Гадасин В. А. Концепция триад – понятие «информация» как субстанция // Ежегодник ВНИИ-ПВТИ: Сб. науч. тр. Минск, 2007. С. 186–190.
5. Григорьев О. Г. Роль и уголовно-процессуальное значение компьютерной информации на досудебных стадиях уголовного судопроизводства: дис. ... канд. юрид. наук. Тюмень, 2003. 221 с.
6. Колин К. К. Философия информации: структура реальности и феномен информации // Метафизика. 2013. № 4 (10). С. 6–84.
7. Корма В. Д. Информационный аспект следственной деятельности // Вестник университета имени О. Е. Кутафина (МГЮА). 2021. № 2 (78). С. 27–36.

¹⁶ Цифровая криминалистика: учебник для вузов; под ред. В. Б. Вехова, С. В. Зуева. М., 2021. С. 71.

8. Ларин Е. Г. Копирование информации с электронных носителей при производстве по уголовному делу // Законодательство и практика. 2012. № 2 (29). С. 52–53.
9. Маслов А. В. Электронная информация, как доказательство по уголовным делам / А. В. Маслов, К. А. Соскова // Центральный научный вестник. 2017. Т. 2, № 11 (28). С. 57–59.
10. Овсянников Д. В. Доказательственное значение результатов копирования электронной информации в уголовном процессе // Правопорядок: история, теория, практика. 2015. № 2 (5). С. 3–36.
11. Поляков М. П. Уголовно-процессуальная интерпретация результатов оперативно-розыскной деятельности: монография. Н. Новгород: Нижегородская правовая академия, 2001. 262 с.
12. Тушев А. А. Информация как основа всех видов доказательств в уголовном процессе / А. А. Тушев, Н. А. Назаров // Общество и право. 2012. № 3 (40). С. 195–197.
13. Хохлов Г. И. Основы теории информации: учеб. пособие. М., 2008. 170 с.
14. Цифровая криминалистика: учебник для вузов / В. Б. Вехов [и др.]; под ред. В. Б. Вехова, С. В. Зуева. М: Издательство Юрайт, 2021. 417 с.
15. Шенон К. Работы по теории информации и кибернетике. М.: Изд. иностр. лит., 1963. 830 с.
16. Шрейдер Ю. А. Об одной модели семантической теории информации // Проблемы кибернетики. 1965. Вып. 3. С. 233–240.
17. Шрейдер Ю. А. Тезаурусы в информатике и логической семантике // Научно-техническая информация. 1971. Сер. 2, № 3. С. 7–12.
18. Яковлева О. А. Классификация криминалистически значимой информации и ее роль в досудебном уголовном производстве // Вестник Волгоградского государственного университета. Серия 5: Юриспруденция. 2016. Т. 15, № 1 (30). С. 189–193.

Sergey V. Zuev

Doctor of Law, Associate Professor,
Professor at the Department of Law Enforcement and National Security,
South Ural State University
(Chelyabinsk, Russian Federation)
zuevsergij@inbox.ru

THE MAIN DIRECTIONS OF CONVERGENCE OF PHYSICS AND LAW IN CRIMINAL PROCEEDINGS UNDER CONDITIONS OF DIGITALIZATION

Abstract: In the article the author states that digitalization leads to convergence of exact sciences and humanities, in particular physics and law in criminal proceedings. Determines the main directions of this phenomenon, which are associated with the development of information relations in the criminal proceedings, with the widespread

use of electronic means of proof in criminal cases, as well as the interaction of material criminal procedure objects.

Keywords: digitalization, criminal procedure, physics, law, electronic information.

УДК 34.343.9

Мазунин Яков Маркиянович

Доктор юридических наук, профессор, профессор кафедры криминалистики,
Омская академия МВД России
(г. Омск, Российская Федерация)
yakovmazunin@yandex.ru

Белова Ксения Сергеевна

Преподаватель кафедры криминалистики,
Омская академия МВД России
(г. Омск, Российская Федерация)
k_s159@mail.ru

ОСОБЕННОСТИ ФИКСАЦИИ ДОПРОСА, ПРОВОДИМОГО С ИСПОЛЬЗОВАНИЕМ ВИДЕОКОНФЕРЕНЦСВЯЗИ

Аннотация: Использование видеоконференцсвязи при производстве допроса является новеллой действующего законодательства, что порождает определённые сложности при его проведении как с процессуальной, так и с тактической точки зрения. В данной статье обозначены способы фиксации допроса, проводимого с использованием видеоконференцсвязи: посредством видеозаписи экрана монитора компьютера следователем; видеозаписи допроса специалистом; комбинированным способом.

Ключевые слова: следователь, допрос, видеоконференцсвязь, фиксация, специалист.

Для цитирования:

Мазунин Я. М., Белова К. С. Особенности фиксации допроса, проводимого с использованием видеоконференцсвязи // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 27–30.

Одним из наиболее распространённых коммуникативных следственных действий является допрос. Допрос, как получение показаний от лиц, обладающих сведениями о преступлении и связанными с ним событиями, представляет собой тактически сложное следственное действие.

Более того, в связи с нормами, внесёнными Федеральным законом от 30.12.2021 № 501-ФЗ «О внесении изменений в уголовно-процессуальный кодекс РФ», позволяющими следователю проводить допрос, очную ставку и предъявление для опознания путём использования систем видеоконференцсвязи, существенно

осложняются отдельные моменты, связанные с его производством.

Ещё задолго до вступления в силу данных изменений учеными осуществлены определённые разработки в области тактики проведения допроса с использованием видеоконференцсвязи¹, что подтверждает необходимость её использования при проведении данного следственного действия в определённых ситуациях.

Дело в том, что следователь, проводя допрос в классической форме, реализует весь потенциал выработанных криминалистической тактикой рекомендаций. Сейчас же, используя видеоконференцсвязь, следователь должен предусмотреть особенности, связанные с фиксацией такого допроса, поскольку данная процедура может существенно отличаться.

По общему правилу, согласно ст. 166 УПК РФ, основной формой фиксации следственного действия является составление протокола. Однако в соответствии с ч. 4 ст. 189.1 УПК РФ, применение видеозаписи в ходе допроса, очной ставки и предъявления для опознания с использованием видеоконференцсвязи является обязательным условием

проведения данных следственных действий.

В связи с этим возникает вопрос относительно технологии применения видеозаписи допроса. Традиционно, видеофиксация осуществляется специалистом, использующим для этого видеокамеру. В ракурсе проведения допроса с использованием видеоконференцсвязи путём использования компьютера или иного устройства, в силу того, что в обозначенной норме отсутствуют уточнения по ведению видеозаписи, представляется возможным производить видеофиксацию следующими способами:

- 1) путём видеозаписи экрана монитора компьютера следователем;
- 2) путём видеозаписи допроса специалистом;
- 3) комбинированным способом.

Первый способ, в рамках которого следователем путём записи экрана монитора компьютера фиксируется процесс допроса, представляется нам довольно эффективным поскольку:

- не требуется привлекать к допросу специалиста и дополнительное техническое средство, производящего видеозапись;
- в ходе видеофиксации чётко отображаются все участники

¹ Желтобрюхов С. П. О необходимости предоставления органу предварительного расследования возможности применения видеоконференц-связи на стадии досудебного производства // Российская юстиция. 2016. № 1. С. 62–64; Кравец Е. Г., Шувалов Н. В. Дистанционные следственные действия сквозь призму применения специальных знаний // Юридическая наука и правоохранительная практика. 2017. № 1 (39). С. 140–144; Смагин П. Г. К вопросу о

возможности дистанционного производства следственных действий // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью: Материалы Всероссийской научно-практической конференции. 2015. С. 309–314; Шагеева Р. М. Об использовании видеоконференц-связи в досудебном производстве по уголовным делам // Правовое государство: теория и практика. 2020. № 4–2 (62). С. 67–76 и др.

следственного действия, их вербальная и невербальная коммуникация в рамках разрешения экрана монитора пользователя;

- есть возможность демонстрировать документы в электронном виде для ознакомления;
- не требуются специальные знания в сфере особенностей видеофиксации следственных действий и т. д.

Недостатком данного способа фиксации, по нашему мнению, является то, что видеозапись экрана по какой-либо причине может не сохраниться на устройстве, или следователь не включит соответствующую функцию.

В рамках второго способа фиксации допроса необходимо привлекать как дополнительного участника следственного действия – специалиста, так и дополнительного технического средства – видеокамеры. В данной ситуации внимание

специалиста должно быть направлено и на следователя, проводящего допрос, и на экран монитора, где отображены другие участники следственного действия, в связи с чем могут возникнуть определённые технические сложности.

Использование комбинированного способа фиксации допроса, включающего видеозапись экрана монитора компьютера, а также запись с помощью видеокамеры специалистом может показаться наиболее эффективным, однако в практической деятельности не всегда имеется возможность привлечения дополнительных сил и средств при производстве следственных действий.

Поэтому, считаем целесообразным, фиксировать допрос путём видеозаписи экрана монитора компьютера следователем. Использование данного способа позволяет в полной мере решить задачу, связанную с фиксацией допроса по видеоконференцсвязи.

Список литературы

1. Желтобрюхов С. П. О необходимости предоставления органу предварительного расследования возможности применения видеоконференц-связи на стадии досудебного производства // Российская юстиция. 2016. № 1. С. 62–64.
2. Кравец Е. Г. Дистанционные следственные действия сквозь призму применения специальных знаний / Е. Г. Кравец, Н. В. Шувалов // Юридическая наука и правоохранительная практика. 2017. № 1 (39). С. 140–144.
3. Смагин П. Г. К вопросу о возможности дистанционного производства следственных действий // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью: Материалы Всероссийской научно-практической конференции. 2015. С. 309–314.
4. Шагеева Р. М. Об использовании видеоконференц-связи в досудебном производстве по уголовным делам // Правовое государство: теория и практика. 2020. № 4–2 (62). С. 67–76.

Yakov M. Mazunin

Doctor of Law, Professor, Professor of the Department of Forensic Science,
Omsk Academy of the Ministry of Internal Affairs of Russia
(Omsk, Russian Federation)
yakovmazunin@yandex.ru

Kseniya S. Belova

Lecturer of the Department of Forensic Science,
Omsk Academy of the Ministry of Internal Affairs of Russia
(Omsk, Russian Federation)
k_s159@mail.u

**FEATURES OF RECORDING THE INTERROGATION CARRIED OUT
USING VIDEO CONFERENCE**

Abstract: The use of videoconferencing during interrogation is a novelty of the current legislation, which creates certain difficulties in its conduct, both from a procedural and tactical point of view. This article outlines the ways of fixing the interrogation conducted using video conferencing: by video recording the screen of the computer monitor by the investigator; by video recording of the interrogation by a specialist; in a combined way.

Keywords: investigator, interrogation, video-conferencing, fixation, specialist.

УДК 34.343.98

Мещеряков Владимир Алексеевич

Доктор юридических наук, профессор, профессор кафедры криминалистики,
Воронежский государственный университет
(г. Воронеж, Российская Федерация)
netshuttle@mail.ru

Цурлуй Олеся Юрьевна

Кандидат юридических наук, доцент, доцент кафедры судебной экспертизы
и криминалистики,
Российский государственный
университет правосудия, Центральный филиал
(г. Воронеж, Российская Федерация)
kijalis@yandex.ru

ДОПРОС В СВЕТЕ ИЗМЕНЕНИЙ, ВНЕСЁННЫХ В УГОЛОВНО-ПРОЦЕССУАЛЬНОЕ ЗАКОНОДАТЕЛЬСТВО В ДЕКАБРЕ 2021 ГОДА

Аннотация: Необходимость законодательной адаптации уголовного судопроизводства к реалиям цифровой среды особенно остро возникла в период ограничений, обусловленных пандемией. В частности, такие изменения требовались в процедуре дистанционного допроса и были внесены законодателем в конце прошлого года. Однако данная законодательная новелла требует осмысления и анализа с точки зрения её реализации и тактики проведения.

Ключевые слова: допрос, цифровые технологии, видео-конференц-связь, тактика допроса, порядок допроса, эффективность допроса

Для цитирования:

Мещеряков В. А., Цурлуй О. Ю. Допрос в свете изменений, внесённых в уголовно-процессуальное законодательство в декабре 2021 года // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 31–38.

В декабре прошлого года в Уголовно-процессуальный кодекс РФ внесена статья 189.1, регламентирующая особенности проведения допроса, очной ставки, опознания путём использования систем видео-конференц-связи. Необходимость дистанционного допроса назрела давно, но данные

изменения во много внесены вынужденно в связи с пандемией Covid-19. Оценивая их в целом положительно, полагаем необходимым указать на ряд дискуссионных моментов.

Федеральный закон предоставляет следователю, дознавателю право самостоятельно

определять основания проведения допроса путём использования систем видео-конференц-связи, при наличии технической возможности по правилам ст. 164 и главы 26 УПК РФ с учётом соответствующих особенностей. Это обоснованно, поскольку в уголовно-процессуальном законе невозможно установить исчерпывающий перечень фактических оснований проведения допроса дистанционно. Думается, что реализация следователем, дознавателем предоставленного законом права возможна и при наличии соответствующего ходатайства лица, вызванного на допрос.

Справедливо в качестве фактических оснований производства допроса путём использования систем видео-конференц-связи обозначить следующие¹:

- невозможность личного присутствия допрашиваемого, обусловленная состоянием здоровья, возрастом, наличием малолетних детей и/или членов семьи, нуждающихся в постоянном уходе, иными уважительными причинами;

- личное присутствие допрашиваемого связано с высокими расходами, например длительная дорогостоящая командировка к месту производства расследования;

- осуществление трудовой деятельности за пределами страны и невозможность прервать её осуществление на длительный срок;

- допросу подлежат свидетели, к которым применяются меры

безопасности в соответствии с ч. 9 ст. 166 УПК РФ;

- допросу подлежит несовершеннолетний свидетель.

Юридическим основанием производства допроса путём использования систем видео-конференц-связи согласно ч. 2 ст. 189.1 УПК РФ является письменное поручение следователя или дознавателя, осуществляющего производство предварительного расследования, об организации участия лица, подлежащего допросу в данном следственном действии, направляемое следователю, дознавателю или в орган дознания по месту нахождения допрашиваемого лица.

Безусловно осуществление в соответствии с ч. 3 ст. 189.1 УПК РФ полномочий по разъяснению прав, обязанностей, ответственности и порядка производства допроса, составлению протокола допроса, записи об оглашении протокола допроса лицу, удостоверяемых подписями допрошенного лица, с отображением у него соответствующей подписи следователем или дознавателем по месту нахождения допрашиваемого лица гарантирует законность и достоверность допроса. Одновременно организационные сложности допроса остаются.

Учитывая современный уровень развития цифровых технологий, в некоторых случаях вполне допустимо производство допроса с

¹ Антонович Е. К. Использование цифровых технологий при допросе свидетелей на досудебных стадиях уголовного судопроизводства (сравнительно-правовой анализ законодательства Российской

Федерации и законодательства некоторых иностранных государств) // Актуальные проблемы российского права. 2019. № 6. С. 129.

использованием систем видео-конференц-связи непосредственно с допрашиваемым лицом, без привлечения следователя, дознавателя по месту нахождения допрашиваемого.

Современный уровень развития информационных технологий позволяет решить вопрос аутентификации (например, по лицу и голосу) участника судебного процесса для дистанционного участия в допросе.

Вполне надёжным способом установления личности допрашиваемого дистанционно выступает предложенный законодателем в проекте № 1144921-7 Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации в части регулирования дистанционного участия в судебном процессе» способ, а именно, использование информационно-технологических средств, обеспечивающих идентификацию лица без его личного присутствия, т. е. единой системы идентификации и аутентификации, единой информационной системы персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации.

Система видео-конференции, в том числе с возможностью биометрической аутентификации, способна обеспечить возможность дистанционного участия в допросе лиц из помещений, расположенных вне

зданий правоохранительных органов или судов, вне зависимости от их местонахождения.

Доступ к системе веб-конференции должен быть обеспечен из личного кабинета Единого портала государственных услуг (ЕПГУ).

Разъяснение следователем, дознавателем прав, обязанностей и ответственности участвующему в допросе лицу могут быть оформлены электронным документом, подписанным усиленной квалифицированной электронной подписью, либо подтверждением может служить видеозапись дистанционного допроса, учитывая, что на основании ч. 4 ст. 189.1 УПК РФ применение видеозаписи в ходе допроса обязательно. Следовательно, дознавателю необходимо обеспечить техническую возможность видеозаписи допроса с приобщением к протоколу соответствующего следственного действия.

Учитывая значимость исправности технических средств для проведения дистанционного допроса, следует заранее протестировать программу, посредством которой будет проходить видео-конференция, предусмотреть альтернативное средство связи в случае сбоя в работе используемого. Полагаем целесообразным будет присутствие при производстве дистанционного допроса специалиста в области компьютерной техники.

В целях предотвращения разглашения данных предварительного расследования и соблюдения требований ст. 161 УПК РФ и ст. 310 УК РФ средство связи, используемое при дистанционном

допросе, должно быть российского производства.

Абсолютно рационально законодателем в ч. 8 ст. 189.1 УПК РФ запрещено проведение допроса путём использования систем видео-конференц-связи в случае возможности разглашения государственной или иной охраняемой федеральным законом тайны либо данных о лице, в отношении которого приняты меры безопасности.

Учитывая, что дистанционный допрос производится с соблюдением требований уголовно-процессуального закона, в перечень обязательных участников допроса с использованием систем видео-конференц-связи включаются адвокат, законный представитель, педагог, психолог, переводчик, специалист. Полагаем, что специалисту следует присутствовать по месту нахождения следователя. Остальным участникам целесообразно присутствовать по месту нахождения допрашиваемого. В целях соблюдения прав и законных интересов подозреваемого и обвиняемого возможно обеспечение участия двух адвокатов-защитников, один из которых присутствует по месту нахождения следователя, второй вместе с подзащитным. Адвокат-представитель может находиться как вместе с доверителем, так и по месту нахождения следователя, на усмотрение доверителя.

Ход и результаты дистанционного допроса, а также показания допрашиваемого дословно фиксируются в протоколе по правилам, предусмотренным ст. ст. 166, 167 УПК РФ. Видеозапись дистанционного допроса подтвердит

при необходимости объективность следственного действия, а также позволит следователю впоследствии просматривать её и анализировать поведение допрашиваемого в целях оценки полученного доказательства. Согласно ч. 5 ст. 189.1 УПК РФ после завершения допроса, проведённого путём использования систем видео-конференц-связи, составления и оглашения протокола допрошенное лицо вправе принести замечания о дополнении и уточнении протокола в подпiske.

На наш взгляд, удостоверение лицом протокола допроса возможно посредством электронной подписи либо устно, что фиксируется видеозаписью допроса, о чём следователь, дознаватель делает отметку в протоколе. Аналогично устно с фиксацией в видеозаписи лицо, участвующее в допросе путём использования систем видео-конференц-связи, вправе подавать заявления и замечания на протокол допроса, подлежащие занесению в протокол, а также ходатайствовать о приобщении документов, которые направляются органу предварительного расследования в электронном виде.

В соответствии с требованиями ч. ч. 6, 7 ст. 189.1 УПК РФ после завершения допроса, проведённого путём использования систем видео-конференц-связи, следователь, дознаватель или орган дознания по месту нахождения допрошенного лица, в течение 24 часов направляет следователю или дознавателю, которым поручено производство предварительного расследования, подписку и приобщённые к ней в ходе

допроса документы и материалы, а также ордер адвоката, в случае его участия, которые приобщаются к протоколу допроса.

Полагаем, что подготовка следователя / дознавателя к дистанционному допросу должна быть надлежащей и включать аналогичный для стандартного допроса перечень действий²:

- выбор времени, способа вызова на допрос;
- подготовка технических средств и программного обеспечения;
- организация оптимальных технических условий для проведения допроса;
- изучение материалов уголовного дела;
- получение при необходимости сведений от сведущего лица по специальным вопросам, связанным с предметом допроса;
- изучение личности допрашиваемого: его характеристик, протоколов допросов родственников, знакомых и т. д.;
- составление плана допроса с конкретным перечнем вопросов, подлежащих выяснению;
- подготовка доказательств, которые могут быть предъявлены при допросе.

Процедура вызова для допроса в дистанционной форме аналогична процедуре вызова для дачи показаний

в стандартном режиме. С учётом изложенного выбор формата допроса определяется уже после уведомления лица о предстоящем следственном действии.

Полагаем, тактические приёмы допроса с использованием систем видео-конференц-связи должны соответствовать требованиям, предъявляемым при проведении допроса в стандартной форме, т. е. «законности, избирательности и этичности»³.

Следователь / дознаватель при проведении дистанционного допроса в обязательном порядке должен учитывать сложившуюся ситуацию: конфликтную или бесконфликтную⁴.

Как отмечалось, общие правила проведения допроса, предусмотренные ст. 189 УПК РФ всецело распространяются на допрос с использованием систем видео-конференц-связи.

Следовательно, выполнив обязательные формальности, «следователь предлагает допрашиваемому рассказать об обстоятельствах, касающихся расследуемого уголовного дела в свободном рассказе. Не рекомендуется прерывать лицо, дающее показания, даже, если следователю уже известны излагаемые факты или если допрашиваемый высказывает ложные

² Криминалистика: учебник для бакалавров и специалистов / Э. У. Бабаева, О. В. Волохова, Н. Н. Егоров [и др.]; отв. ред. д.ю.н., проф. Е. П. Ищенко. М.: Проспект, 2020. С. 134.

³ Баев М. О., Баев О. Я. Тактика уголовного преследования и профессиональной защиты от него: Прокурорская тактика. Адвокатская

тактика: Научно-практическое пособие. М.: Экзамен, 2005. 318 с.

⁴ Руководство для государственного обвинителя: учебное пособие / Л. Т. Волнянская, Н. А. Данилова, С. Г. Евдокимов [и др.]; под ред. О. Н. Коршуновой. 4-е изд., испр. и доп. М.: Юстиция, 2019. 628 с.

сведения»⁵, однако целесообразно напомнить о предмете допроса в случае существенного отклонения допрашиваемого.

В тактически обоснованных ситуациях после свободного рассказа следует вопросно-ответный этап, в ходе которого применяются тактические приёмы, обусловленные сложившейся следственной ситуацией и процессуальным положением допрашиваемого, сведениями о его личности, спецификой расследуемого преступления с обязательным недопущением постановки наводящих вопросов, применения недопустимых приёмов ведения следствия в виде угроз, физического или психического насилия, унижения чести и достоинства и др.

Требования, предъявляемые к вопросам, задаваемым в ходе дистанционного допроса: вопрос может быть спонтанным, представляющим собой немедленную ответную реакцию следователя на слова, действия, иные проявления активности допрашиваемого в тот или иной момент допроса; заранее обдуманым, вербально, технически, тактически и организационно подготовленным; адресным, лаконичным, корректным, понятным носителю информации; не должен содержать подсказку, быть наводящим.

Наблюдение за допрашиваемым в ходе его ответа на вопросы следователя на наш взгляд может быть

затруднено при использовании систем видео-конференц-связи, поскольку восприятие человека через экран несколько отличается от живого общения. Например, заметить изменения в поведении допрашиваемого вполне возможно, как и в настроении, но вот внешние проявления – изменение цвета кожных покровов, тремор рук – увидеть в формате онлайн сложно. Однако это не исключает необходимость использования следователем / дознавателем данного тактического приёма.

В целях активации памяти допрашиваемого его следует ознакомить с фрагментами показаний других лиц, предъявить фотографии, планы, схемы объекты, вещественные доказательства, если следователь, дознаватель сочтёт такой приём тактически целесообразным. При этом следует осуществлять непрерывное наблюдение за допрашиваемым в момент предъявления, чтобы заметить его реакцию. В таких ситуациях следователю может понадобиться помощь специалиста, обеспечивающего техническую сторону дистанционного допроса.

Полагаем, что разработанные наукой криминалистикой принципы допроса⁶ следует обязательно применять и в ходе проведения допроса дистанционно, поскольку они способствуют эффективности данного следственного действия:

⁵ Криминалистика: учебник для бакалавров и специалистов / Э. У. Бабаева, О. В. Волохова, Н. Н. Егоров [и др.]; отв. ред. д.ю.н., проф. Е. П. Ищенко. М.: Проспект, 2020. 560 с.

⁶ Сажаяев А. М., Мишуточкин А. Л. О некоторых особенностях тактики допроса свидетелей // Расследование преступлений: проблемы и пути их решения. 2020. № 4. С. 103–106.

- строго индивидуальный подход к каждому лицу, дающему показания, учёт индивидуальных особенностей личности, криминалистической ситуации, а также места и роли допрашиваемого в познаваемой по делу ситуации;

- создание до и во время допроса предпосылок, обеспечивающих свободу волеизъявления допрашиваемого лица, полную реализацию его прав, обязанностей и возможности дать исчерпывающие, правдивые показания;

- целеустремленный, активный, наступательный характер допроса;

- чёткость, полнота, объективность фиксации задаваемых вопросов и информации, полученной от допрашиваемого, на основе безусловного выполнения нормативных требований данного процесса;

- обеспечение критического анализа, тактически правильной

оценки показаний допрашиваемого лица.

Внедрение в уголовно-процессуальный закон РФ процедуры допроса путём использования систем видео-конференц-связи с обязательным участием следователя, дознавателя по месту нахождения допрашиваемого лица обусловлена спецификой, многогранностью, сложностью уголовно-процессуальной деятельности, высоким риском нарушения прав и свобод участников судопроизводства, неготовностью общества и профессионального сообщества использовать цифровые технологии без участия человека.

Безусловно, основная идея в том, что следователь, дознаватель вправе отказаться от проведения допроса с использованием систем видео-конференц-связи в случаях наличия достаточных оснований полагать, что дистанционная форма допроса не обеспечит его эффективности и получение достоверных показаний.

Список литературы

1. Антонович Е. К. Использование цифровых технологий при допросе свидетелей на досудебных стадиях уголовного судопроизводства (сравнительно-правовой анализ законодательства Российской Федерации и законодательства некоторых иностранных государств) // Актуальные проблемы российского права. 2019. № 6.

2. Баев М. О. Тактика уголовного преследования и профессиональной защиты от него: Прокурорская тактика. Адвокатская тактика: Научно-практическое пособие / М. О. Баев, О. Я. Баев. М.: Экзамен, 2005. 318 с.

3. Криминалистика: учебник для бакалавров / А. В. Метелев, В. А. Образцов, В. М. Поздняков [и др.]; под ред. д.ю.н., проф. Л. В. Бертовского. М.: Проспект, 2018. 960 с.

4. Криминалистика: учебник для бакалавров и специалистов / Э. У. Бабаева, О. В. Волохова, Н. Н. Егоров [и др.]; отв. ред. д.ю.н., проф. Е. П. Ищенко. М.: Проспект, 2020. 560 с.

5. Руководство для государственного обвинителя: учебное пособие / Л. Т. Волнянская, Н. А. Данилова, С. Г. Евдокимов [и др.]; под ред. О.Н. Коршуновой. 4-е изд., испр. и доп. М.: Юстиция, 2019. 628 с.

6. Сажаев А. М. О некоторых особенностях тактики допроса свидетелей / А. М. Сажаев, А. Л. Мишуточкин // Расследование преступлений: проблемы и пути их решения. 2020. № 4. С. 103–106.

Vladimir A. Meshcheryakov

Doctor of Law, Professor, Professor of the Department of Criminalistics,
Voronezh State University
(Voronezh, Russian Federation)
netshuttle@mail.ru

Olesya Y. Tsurlui

PhD (Law), Associate Professor, Associate Professor of the Department of Forensic
Examination and Criminalistics,
Russian State University of Justice, Central Branch
(Voronezh, Russian Federation)
kijalis@yandex.ru

**INTERROGATION DUE TO THE AMENDMENTS OF CRIMINAL
PROCEDURE LAW OF THE RUSSIAN FEDERATION BY FEDERAL LAW
NO. 501-FZ OF DECEMBER 30, 2021**

Abstract: The need for legislative adaptation of criminal proceedings to the realities of the digital environment has become especially acute during the period of restrictions caused by the pandemic. In particular such changes were required in the remote interrogation procedure and were introduced by the legislator at the end of last year. However, this legislative novelty requires reflection and analysis as its procedure as tactics.

Keywords: interrogation, digital technologies, video conferencing, interrogation tactics, interrogation procedure, interrogation efficiency.

УДК 343.98

Смахтин Евгений Владимирович

Доктор юридических наук, профессор, профессор кафедры криминалистики,
Уральский государственный юридический университет
имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
smaxt@yandex.ru

ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ФОРМИРОВАНИЯ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ И ИХ ПРЕДСТАВЛЕНИЕ В СУД ПЕРВОЙ ИНСТАНЦИИ

Аннотация: В статье рассмотрены процессуальные и тактические вопросы, связанные с формированием электронных доказательств. По мнению автора, электронные носители информации, в случае соблюдения необходимых процедур, предусмотренных уголовно-процессуальным законодательством, трансформируются в электронные доказательства. Процесс формирования электронных доказательств представляет научный интерес не только для уголовно-процессуальной науки, но и для криминалистики, с точки зрения тактики их формирования и использования. Актуальность электронных доказательств обусловлена широким внедрением информационных технологий в уголовное судопроизводство и их объективным характером.

Ключевые слова: информационные технологии, электронные носители информации, электронные доказательства, тактическая операция, тактическая комбинация, судебная ситуация.

Для цитирования:

Смахтин Е. В. Тактические особенности формирования электронных доказательств и их представление в суд первой инстанции // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 39–46.

Последние изменения в уголовно-процессуальном законодательстве довольно часто связаны с развитием информационных технологий. Например, федеральным законом от 30 декабря 2021 № 501-ФЗ внесены изменения, в т. ч. касающиеся дополнения УПК РФ статьёй 189.1, которая регламентирует особенности проведения допроса, очной ставки,

опознания путём использования систем видеоконференцсвязи в досудебном производстве. Развитие в общей системе следственных действий, процессуальных действий, совершаемых с применением информационных технологий, предопределяет необходимость уточнения тактических средств, связанных с движением

криминалистически значимой информации на различных стадиях уголовного судопроизводства.

В настоящее время с применением информационных технологий следователем могут быть получены практически все известные виды доказательств. Не менее важно и то, что рассматриваемые технологии используются в ходе оперативно-розыскной деятельности, результаты которой представляются следователю и могут быть задействованы в доказывании по уголовному делу.

Научные исследования и учебно-методические работы, связанные с т. н. электронными доказательствами в уголовном судопроизводстве, в последнее время приобретают всё большую актуальность¹.

Представляется, что важной на сегодняшний день научной проблемой является и исследование тактических аспектов, связанных с движением электронной информации в уголовном судопроизводстве. Законодатель не использует термин электронные доказательства, поэтому полагаем, что на них распространяется тот же процессуальный режим, что и на обычные. Вместе с тем, во многих статьях УПК РФ используется словосочетание электронные носители информации. Рассмотрим трансформацию электронных носителей информации в электронные доказательства.

Любые электронные носители информации в уголовном судопроизводстве после их процессуального закрепления приобретают статус доказательств. Это могут быть вещественные доказательства и документы. Они могут содержать сведения, зафиксированные на различных цифровых носителях информации, а также в обычных процессуальных документах.

Цифровые носители информации используются при производстве допросов, очных ставок, опознания (фото-, видеофиксация, видеоконференцсвязь и пр.), особенно после дополнения УПК РФ статьёй 189.1. Полученные цифровые материалы, если они не имеют самостоятельного процессуального характера, прилагаются к протоколам следственных действий, соответственно, хранятся в уголовном деле. Соответственно, логично утверждать, что электронные носители после обретения процессуального статуса могут именоваться электронными доказательствами.

После завершения предварительного расследования уголовное дело направляется в суд для его рассмотрения по существу. Суд в ходе первого судебного заседания решает ряд важных процессуальных вопросов, в том числе определяет порядок исследования доказательств.

¹ Основы теории электронных доказательств: монография / А. Н. Балашов [и др.]; под ред. С. В. Зуева. Москва: Юрлитинформ, 2019. 400 с.; Развитие информационных технологий в уголовном судопроизводстве: монография / В. С. Балакшин [и др.]; под ред. С. В. Зуева. Москва: Юрлитинформ, 2018.

248 с.; Электронные носители информации в криминалистике: монография / отв. ред. О. С. Кучин. Москва: Юрлитинформ, 2017. 304 с.; IT-справочник следователя / В. Б. Вехов [и др.]; под ред. С. В. Зуева. Москва: Юрлитинформ, 2019. 232 с.

На наш взгляд, УПК регламентирует лишь очерёдность исследования доказательств: сначала предоставленные стороной обвинения, а затем – стороной защиты. Следовательно, участники уголовного судопроизводства свободны в выборе тактики представления доказательств суду². Важным в этом отношении является определение очерёдности (последовательности) исследования доказательств внутри указанных групп. Это относится и к электронным доказательствам.

Общеизвестно, что криминалистическая тактика – это раздел криминалистики, в котором изучаются закономерности организации и ведения не только досудебного, но судебного производств³. Об использовании тех или иных тактических средств принимается тактическое решение, которое представляет собой результат интеллектуальной оценки целей и задач, обусловленных криминалистической ситуацией, складывающейся по делу, и последующее волевое действие, направленное на её изменение в благоприятную сторону.

С точки зрения последовательности работы с доказательствами, в том числе электронными, можно выделить:

- тактику собирания и проверки электронных доказательств;

- тактику анализа и оценки электронных доказательств;

- тактику использования электронных доказательств в уголовном судопроизводстве.

Поскольку мы рассматриваем досудебное и судебное производства, можно выделить комплексные тактические средства, которые применимы на обеих стадиях.

В тех случаях, когда тактических средств недостаточно, привлекаются субъекты оперативно-розыскной деятельности, которые в рамках полномочий могут представить результаты своей работы, проводимой, как правило, в ходе тактических операций⁴.

Тактические средства судебного производства достаточно разнообразны. К началу судебного следствия участники процесса могут совершенно по-разному оценивать актуальную ситуацию по делу.

В простых судебных ситуациях, государственный обвинитель, как правило, предлагает допросить потерпевшего, при его наличии, свидетелей, а затем перейти к исследованию материалов уголовного дела. В этом случае подсудимый допрашивается в конце судебного следствия. Затем очередь переходит к выступлению стороны защиты. Доказательства представляются как на бумажных, так и на электронных носителях информации. Однако в этой ситуации, электронные

² Цифровая криминалистика: учебник для вузов / В. Б. Вехов [и др.]; под ред. В. Б. Вехова, С. В. Зуева. Москва: Юрайт, 2021. С. 269–281.

³ См.: Криминалистика: учебник для вузов. / К. Г. Иванов [и др.]; под научной редакцией

В. Н. Карагодина, Е. В. Смахина. 2 изд. Москва: Издательство Юрайт, 2020. С. 184.

⁴ См. подр. об этом: Криминалистика: учебник / под науч. ред. В. Н. Карагодина, Е. В. Смахина. Тюмень: Издательство ТюмГУ, 2018. С. 253–258.

доказательства, как правило, не исследуются, суд ограничивается изучением материалов уголовного дела. Если сторона защиты также полагает, что судебная ситуация простая, она соглашается с порядком исследования доказательств, а имеющиеся в деле электронные материалы предлагает изучить, если в этом возникнет необходимость.

В некоторых простых ситуациях, когда обвиняемый полностью признаёт свою вину, вред возмещён, он, по согласованию со всеми участниками уголовного судопроизводства, может быть допрошен в первую очередь.

Обычно при представлении и исследовании в суде электронных носителей информации особых сложностей не возникает. Весь процесс связан, например, с прослушиванием фонограммы и сравнением её с показаниями, зафиксированными в протоколе допроса.

Здесь же возможны случаи оглашения показаний неявившихся свидетелей. Тогда после их прочтения из протоколов допроса, сторона, заявившая ходатайство об оглашении, может представить к воспроизведению и цифровые носители информации.

Есть и более сложные ситуации, связанные с использованием информационных технологий в ходе рассмотрения дела по существу.

В ряде случаев суд не может провести допрос свидетеля, а против оглашения его показаний возражает одна из сторон. Тогда возможно допросить неявившегося свидетеля с использованием средств видеоконференцсвязи. Наибольшие тактические сложности возникают в ходе организации взаимодействия с

судом по месту нахождения свидетеля. После осуществления организационно-тактических действий, связанных с подготовкой процессуального действия, суд по месту нахождения свидетеля осуществляет свои процессуальные полномочия, предусмотренные ст. 278.1 УПК РФ. С точки зрения криминалистики интерес представляют вопросы, которые будут заданы свидетелю и могут содержать в себе различные по своему наполнению тактические аспекты. Так, одни из них могут быть направлены на детализацию показаний, другие – на разъяснение ошибочности избранной позиции и повторение показаний, данных на предварительном следствии и т. п. Зачастую, в такой судебной ситуации осуществляется демонстрация электронной информации на цифровых носителях, являющихся приложением протокола допроса свидетеля.

При возникновении ситуации, связанной с необходимостью допроса эксперта в судебном заседании, стороны ходатайствуют об этом. С точки зрения тактики важно, что эксперт может предоставить суду не только свои разъяснения и дополнения, но и другие сведения, в том числе на цифровых носителях информации. В тех случаях, когда электронные носители информации имеют значение для дела, они приобщаются судом к материалам уголовного дела, а самим источникам даётся оценка в итоговом судебном решении. Если же эксперт, допрошенный в судебном заседании, по каким-либо причинам не смог разъяснить своё заключение, не ответил на вопросы, заданные

участниками уголовного процесса, по существу, возникает процессуальная и тактическая потребность назначения дополнительной или повторной экспертиз. После поступления в суд нового доказательства, в том числе, содержащего приложения на цифровых носителях информации, оно исследуется по общим правилам работы с доказательствами, с точки зрения их проверки и оценки.

Сложные судебные ситуации достаточно разнообразны. За основу в настоящей статье возьмём их классификацию, предложенную Л. Я. Драпкиным. В зависимости от сути острого соперничества, либо конфликта, возникают различные комбинации сложных ситуаций, в данном случае судебных. Пробелы в расследовании, процессуальные и тактические ошибки приводят к организационно-неупорядоченным и даже тупиковым ситуациям. Возможны и их различные сочетания⁵.

На наш взгляд, наибольший интерес представляют тактические особенности представления электронных носителей информации в комбинированной судебной ситуации с элементами острого соперничества, конфликта, процессуальных и тактических ошибок.

Например, в сложной комбинированной судебной ситуации, когда по уголовному делу изъято большое количество электронных носителей информации, признанных вещественными доказательствами и иными документами, прокурор может

предложить особую последовательность их исследования. В этом случае, в целях наиболее эффективной организации судебного следствия, прокурор может начать судебное следствие, например, с допроса потерпевшего, а затем – исследовать все электронные носители информации, полученные с его участием. Это позволит тактически верно оценить правдивость показаний потерпевшего, восполнить пробелы в них и т. п. Затем, после допроса свидетелей, государственный обвинитель также может ходатайствовать об исследовании электронных носителей информации, изъятых у допрашиваемых свидетелей. После исследования и оглашения остальных материалов уголовного дела, допроса подсудимого, также исследуются электронные носители информации, изъятые у подсудимого или с его участием. Такой порядок наиболее эффективен, когда рассматриваются большие по объёму уголовные дела. Если же для данного вида ситуаций был избран традиционный порядок исследования доказательств, после допросов в суде участников уголовного судопроизводства и оглашения документов, возникает необходимость в их повторных допросах для устранения противоречий, имеющих в показаниях и электронных носителях информации, которые на наш взгляд, носят более объективный характер. Эти негативные обстоятельства ведут к значительному увеличению сроков

⁵ Драпкин Л. Я. Основы теории следственных ситуаций. Свердловск: Издательство Уральского ун-та, 1987. 164 с.

судебного следствия, которое может длиться многие месяцы и даже годы, и свидетельствуют о тактических просчётах государственного обвинения.

Завершив исследование электронных доказательств, в том числе полученных в ходе оперативно-розыскной деятельности и трансформированных в доказательства, суд по собственной инициативе, либо по ходатайству одной из сторон, вправе потребовать представить результаты проведённых дополнительно оперативно-розыскных мероприятий, которые были получены после направления уголовного дела в суд. Такие ситуации возможны, когда имеющихся в уголовном деле доказательств недостаточно для принятия законного, обоснованного и справедливого решения.

В этом случае оперативно-розыскные мероприятия проводятся чаще всего с помощью информационных технологий, их результаты также нередко закрепляются не на бумажных, а на электронных носителях, что, в совокупности, позволяет нам считать такие комбинированные ситуации наиболее сложными.

Уточним, что в данном случае мы рассматриваем трансформацию электронных носителей информации, полученных оперативно-розыскным путём в электронные доказательства. Первичную информацию оперативно-розыскного характера участниками процесса необходимо будет проверить и оценить, придать ей необходимую

процессуальную форму. Напрямую использование результатов оперативно-розыскной деятельности в уголовном судопроизводстве недопустимо.

Мы разделяем позицию А. И. Зазулина, который исследовал вопросы, связанные с использованием цифровой информации в доказывании по уголовным делам⁶. Из выводов учёного следует, что по своей природе результаты оперативно-розыскной деятельности служат вспомогательным средством, позволяющим установить конкретные обстоятельства, и не могут подменять фактические данные, получаемые и подтверждаемые в уголовно-процессуальных процедурах, обеспечивающих допустимость и достоверность добытых сведений, возможность их проверки и оценки.

В рассматриваемой ситуации для представления результатов оперативно-розыскной деятельности необходим ряд документов (рапорт на имя руководителя органа, осуществляющего оперативно-розыскную деятельность; постановление руководителя органа о представлении результатов оперативно-розыскной деятельности в суд, а также постановление о их рассекретивании). К представляемым документам прилагаются бумажные и цифровые носители (CD-диск, флеш-накопитель и т. п.).

После представления результатов оперативно-розыскной деятельности в суд, прокурор предлагает порядок их исследования. С

⁶ См.: Зазулин А. И. Использование цифровой информации в доказывании по уголовным

делам: монография. Москва: Юрлитинформ, 2019. 168 с.

процессуальной и тактической точки зрения необходима проверка и оценка полученных результатов на предмет их относимости, допустимости и достоверности. Полученные сведения должны согласовываться, сопоставляться с другими доказательствами, которые ранее исследовались в ходе судебного следствия.

В результате оценки полученных результатов суд отражает их основное содержание в протоколе судебного заседания, а в приговоре либо ином итоговом решении даёт оценку всем исследованным в ходе судебного следствия электронным доказательствам. В тех случаях, когда представленные результаты не обладают требуемыми свойствами, они исключаются из числа

доказательств, что также должно найти своё отражение в судебном решении.

Полагаем, что в процессе трансформации электронных носителей информации в электронные доказательства происходит т. н. процесс формирования доказательств. Нередко в настоящее время именно электронные доказательства выступают в качестве объективных источников информации.

Краткий анализ рассматриваемого процесса с точки зрения криминалистической тактики позволяет прийти к выводу о том, что во всех судебных ситуациях процесс перехода от электронной информации к электронному доказательству осуществляется в форме тактических комбинаций и тактических операций.

Список литературы

1. Драпкин Л. Я. Основы теории следственных ситуаций. Свердловск: Издательство Уральского ун-та, 1987. 164 с.
2. Зазулин А. И. Использование цифровой информации в доказывании по уголовным делам: монография. Москва: Юрлитинформ, 2019. 168 с.
3. Криминалистика: учебник / под науч. ред. В. Н. Карагодина, Е. В. Смахина. Тюмень: Издательство ТюмГУ, 2018. 487 с.
4. Криминалистика: учебник для вузов / К. Г. Иванов [и др.]; под науч. ред. В. Н. Карагодина, Е. В. Смахина. 2 изд. Москва: Издательство Юрайт, 2020. 487 с.
5. Основы теории электронных доказательств: монография. / А. Н. Балашов [и др.]; под ред. С. В. Зуева. Москва: Юрлитинформ, 2019. 400 с.
6. Развитие информационных технологий в уголовном судопроизводстве: монография. / В. С. Балакшин [и др.]; под ред. С. В. Зуева. Москва: Юрлитинформ, 2018. 248 с.
7. Цифровая криминалистика: учебник для вузов / В. Б. Вехов [и др.]; под ред. В. Б. Вехова, С. В. Зуева. Москва: Юрайт, 2021. 417 с.
8. Электронные носители информации в криминалистике: монография / отв. ред. О. С. Кучин. Москва: Юрлитинформ, 2017. 304 с.
9. IT-справочник следователя / В. Б. Вехов [и др.]; под ред. С. В. Зуева. Москва: Юрлитинформ, 2019. 232 с.

Evgeny V. Smakhtin

Doctor of Law, Professor, Professor of the Department of Criminalistics,
Ural State Law University
named after V.F. Yakovlev
(Yekaterinburg, Russian Federation)
smaxt@yandex.ru

TACTICAL PECULIARITIES OF FORMATION OF ELECTRONIC EVIDENCE AND ITS PRESENTATION TO THE COURT OF FIRST INSTANCE

Abstract: The article discusses procedural and tactical issues related to the formation of electronic evidence. According to the author, electronic media, in case of compliance with the necessary procedures provided for by the criminal procedure legislation, are transformed into electronic evidence. The process of forming electronic evidence is of scientific interest not only for criminal procedure science, but also criminalistics, from the point of view of tactics of formation and use of electronic evidence. The relevance of electronic evidence is due to the widespread introduction of information technologies in criminal proceedings and their objective nature.

Keywords: information technology, electronic media, electronic evidence, tactical operation, tactical combination, judicial situation.

УДК 343.98

Бахтеев Дмитрий Валерьевич

Кандидат юридических наук, доцент

доцент кафедры криминалистики,

Уральский государственный юридический университет

имени В. Ф. Яковлева

(г. Екатеринбург, Российская Федерация)

ae@crimlib.info

ТАКТИКА ИСПОЛЬЗОВАНИЯ ДРОНОВ ПРИ ОСМОТРЕ МЕСТА ПРОИСШЕСТВИЯ

Аннотация: В статье рассматриваются тактические возможности использования беспилотных летательных аппаратов при осмотре мест происшествий. Характеризуются ситуации осмотра трупа, самодельных взрывных устройств, мест происшествия при падении человека с высоты или падения объектов (например, снега) на человека, при формировании трёхмерных панорам и графических моделей местности. Оцениваются технические риски при использовании дронов.

Ключевые слова: дрон, квадрокоптер, БПЛА, криминалистика, осмотр места происшествия, осмотр трупа.

Для цитирования:

Бахтеев Д. В. Тактика использования дронов при осмотре места происшествия // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 47–51.

Развитие технологий аккумуляторных батарей, видеокамер и радиосвязи привело к появлению современного класса технических средств – дронов, позволяющих без особых финансовых затрат обеспечивать наблюдение и фиксацию окружающей обстановки с большой высоты, что вполне соответствует задачам, разрешаемым следователем на месте происшествия. Ещё

Р. С. Белкин при описании теоретических основ криминалистики упоминал закон активного творческого приспособления криминалистикой для целей судопроизводства достижений различных наук¹. Одни технологии создают новые направления в работе человека, другие – оптимизируют отдельные аспекты профессиональной деятельности. В данной статье мы попробуем проанализировать

¹ Белкин Р. С. Курс криминалистики. Учебное пособие для вузов в 3-х томах. Т. 1. 3-е изд., дополненное, 2001. С. 184.

ситуацию второй группы, а именно – возможности использования беспилотных летательных аппаратов как развития судебной фотографии и видеозаписи в следственных действиях.

В статье используется личный опыт автора, его коллег, а также статистические материалы, собранные автором в процессе анкетирования 211 следственных сотрудников Следственного комитета и Полиции России, проходящих службу в 19 регионах Российской Федерации. Большинство респондентов были из Свердловской, Челябинской областей, Краснодарского и Хабаровского краёв.

С 2017 года в России действует Национальный стандарт Российской Федерации ГОСТ Р 57258-2016 «Системы беспилотные авиационные. Термины и определения». Так, беспилотное воздушное судно (unmanned aircraft) определяется как воздушное судно, управляемое в полёте пилотом, находящимся вне борта такого воздушного судна, или выполняющее автономный полёт по заданному предварительно маршруту. В практической деятельности и научных исследованиях встречаются также аббревиатура БПЛА (БЛА), термины «квадрокоптер»² и «дрон». В данной статье мы будем использовать эти термины как взаимозаменяемые, хотя между ними есть определённые различия: так, квадрокоптер имеет строго четыре несущих винта, вращающихся попарно в противоположных направлениях, однако существуют и мультикоптеры с

большим количеством несущих винтов. Дрон, в свою очередь, может пониматься как наземный или водный автономный или дистанционно управляемый объект.

Дроны используются при исследовании обстановки открытых мест происшествий. Типичные ситуации, вызывающие нужду в них, связаны с расследованием техногенных и экологических катастроф, дорожно-транспортных, авиационных и железнодорожных происшествий, однако дроны могут (и по мнению автора, должны) использоваться при любых осмотрах действий на открытой местности, поскольку это позволяет единым кадром охватить всю обстановку места происшествия (или по крайней мере большую её часть), тем самым обеспечив следователя более точным пониманием картины результатов произошедшего события.

Дроны как технико-криминалистическое средство, характеризуются следующими признаками:

1. Низкая стоимость. Учитывая, что альтернативные методы съёмки предполагают использование вертолётных или автоколёсчатых подъёмников, многократное использование небольшого дрона может обойтись государственному бюджету дешевле, чем один вылет вертолётного.

2. Высокая манёвренность: дроны могут использоваться как на открытом пространстве, так и в плотной городской застройке.

² Отметим, что упомянутый ГОСТ предполагает написание этого термина как «квадрАкоптер».

3. Невысокие требования к квалификации оператора: современные дроны способны автономно избегать столкновения с препятствием, следовать за оператором, совершать сложные манёвры. Решение криминалистических задач не требует больших скоростей, поэтому риск столкновения дрона с объектами на месте происшествия при корректном управлении минимален.

4. Быстрая скорость использования. Современные дроны из транспортного состояния приводятся в готовность за несколько минут.

Помимо осмотров больших площадей, дроны могут использоваться и в относительно ограниченном пространстве в следующих ситуациях.

1. Осмотр трупа, находящегося в горизонтальном положении. Проблема фотографирования таких трупов известна ещё с XIX века, когда для её решения использовались методы панорамирования, либо конструкции, подобные изобретённой А. Бертильоном, представлявшие собой штатив для поднятия аппарата на высоту около двух метров, с которой было возможно сделать снимок тела единым кадром. Аналогичным образом можно использовать БПЛА. Следует, однако, учитывать, что современные дроны имеют достаточно большую мощность и создают вокруг себя поток воздуха, который может повредить или переместить небольшие объекты или следы, находящиеся на трупе или рядом с ним.

2. Осмотр самодельных взрывных устройств. Использование дронов является компромиссом между задачей взрывотехника не допустить присутствия человека рядом с таким опасным объектом и желанием следователя осмотреть СВУ до его уничтожения. Облёт СВУ на дроне часто осуществляется уже на взрывотехническом полигоне, так что осмотр с помощью БПЛА может оказаться последней возможностью получить достоверную информацию о внешнем виде СВУ. В этом случае также имеет место фактор риска: современные дроны управляются с помощью радиосигнала и нельзя исключать срабатывание взрывного устройства, имеющего взрыватель на радиоуправлении.

3. Осмотр мест происшествия при падении человека с высоты или падения объектов (например, снега) на человека. Качественная фотосъёмка в таких ситуациях предполагает не только снимки тела, находящегося на поверхности, но и фиксацию траектории падения снизу и сверху, изготовление вертикальной панорамы. Снимки с верхнего ракурса в случаях городской многоэтажной застройки делаются с чердака, крыши (при падении снега), либо с точки, откуда произошло падение человека. Снимки вертикальной панорамы изготавливают с помощью подъёмников или, при наличии высокого строения напротив, – через его окна или балконы. Оба этих способа могут вызвать затруднения: либо связанные с межведомственным взаимодействием (подъёмники используются обычно Государственной противопожарной

службой и применение их для иных задач ведомственными документами не предусмотрено), либо с логистическими проблемами: получением ключей от чердака или крыши и т. п. БПЛА могут стать решением всех приведённых трудностей: современные дроны легко справляются с задачей вертикального взлёта и фотографирования объектов, находящихся под ними.

4. Дроны могут использоваться при формировании трёхмерных панорам и графических моделей местности. Такие объекты могут использоваться при визуализации криминалистически значимой информации: так, «аппаратный комплекс «РАКУРС» позволяет с помощью программного обеспечения выполнять измерения и производить построение схем по фотоснимкам, с максимальной точностью и минимальными временными затратами»³.

Представленные частные задачи разрешимы с помощью сверхкомпактных дронов, подготовка к полёту которых может уложиться в несколько минут.

Полученные с помощью дронов снимки становятся важной частью иллюстрационной таблицы, по сути, расширяя ракурс восприятия следователя и поднимая фотокамеру на метры и десятки метров вверх.

Съёмка с БПЛА является логическим и более доступным

продолжением аэрофотосъёмки с использованием вертолётной, не требующей сложной подготовки: обучающиеся, по преподавательскому опыту автора статьи, осваивают менее чем за час базовые операции по управлению квадрокоптером в целях фотофиксации статичных объектов на месте происшествия на открытой местности. Вместе с тем, из числа опрошенных следователей опыт использования дронов при осмотре места происшествия имеют лишь 18 % респондентов.

При использовании БПЛА сотрудники следственных органов могут столкнуться с проблемой нормативного характера в виде ограничения полётов на определённых территориях или необходимости регистрации таких устройств, получения разрешения на полёт. Согласимся с мнением А. Ю. Шапошникова и Д. Н. Овакимян, согласно которому такие трудности «могут быть легко решены внесением изменений в действующее законодательство, например посредством создания упрощённой процедуры уведомления о полётах при производстве следственных действий или вовсе её отмены, с возложением на соответствующий орган ответственности за обеспечение безопасности полёта»⁴.

Подводя итог, отметим, что беспилотные летательные аппараты, особенно небольших размеров, могут и

³ Рывкин С. Ю. Инновационные аспекты и тенденции тактики производства осмотров с использованием беспилотных авиационных средств // Современный ученый. 2019. № 6. С. 269–279.

⁴ Шапошников А. Ю., Овакимян Д. Н. Применение современных технологий фиксации информации и беспилотных систем при производстве осмотра места происшествия // Судебная власть и уголовный процесс. 2021. № 1. С. 143.

должны использоваться при осмотре мест происшествия, не только в отношении протяжённых по размерам мест, но и в ситуациях осмотра относительно небольших мест происшествия на открытой местности. Это техническое средство, по сути,

являясь промежуточным звеном между штативом и вертолётom, позволяет снизить временные затраты на изготовление качественных снимков места происшествия, значительно расширяя возможности следователя и криминалиста по его изучению.

Список литературы

1. Белкин Р. С. Курс криминалистики. Учебное пособие для вузов в 3-х томах. Т. 1. 3-е изд., дополненное, 2001. 835 с.
2. Рывкин С. Ю. Инновационные аспекты и тенденции тактики производства осмотров с использованием беспилотных авиационных средств // Современный ученый. 2019. № 6. С. 269–279.
3. Шапошников А. Ю. Применение современных технологий фиксации информации и беспилотных систем при производстве осмотра места происшествия / А. Ю. Шапошников, Д. Н. Овакимян // Судебная власть и уголовный процесс. 2021. № 1. С. 142–153.

Dmitry V. Bakhteev

PhD (Law), Associate Professor,
Associate Professor at the Criminalistics Department,
Ural State University of Law named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
ae@crimlib.info

TACTICS OF USING DRONES DURING OF CRIME SCENE INSPECTION

Abstract: The article deals with tactical possibilities of using drones while examining the places of accidents. Situations of corpse inspection, improvised explosive devices, accident scenes when a person falls from a height or objects (e.g., snow) fall on a person, when forming three-dimensional panoramas and graphic models of the area are characterized. The technical risks of using drones are assessed.

Keywords: drone, quadcopter, UAV, criminalistics, inspection of crime scene, inspection of the corpse.

Хамидуллин Руслан Сибагатуллович

Кандидат юридических наук,
начальник кафедры оперативно-разыскной деятельности
Уральский юридический институт МВД России
(г. Екатеринбург, Российская Федерация)
Rkhamidullin30@mvd.ru

**КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОТИВОДЕЙСТВИЯ
НЕЗАКОННОМУ ОБОРОТУ НАРКОТИЧЕСКИХ СРЕДСТВ И
ПСИХОТРОПНЫХ ВЕЩЕСТВ, ОСУЩЕСТВЛЯЕМОМУ В
КРИПТОВАЛЮТЕ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ
«BLOCKCHAIN»**

Аннотация: В данной статье рассмотрены проблемы выявления, раскрытия и расследования преступлений в сфере незаконного оборота наркотиков, осуществляемых в криптовалюте с использованием технологий «blockchain». Проведен анализ некоторых особенностей использования теневого сегмента сети Интернет «DarkNet» с целью незаконного оборота наркотиков. В исследовании особое внимание уделяется криминалистическому обеспечению противодействия обороту наркотических средств, совершаемых дистанционным и бесконтактным способом. Предложены методы и приемы выявления, фиксации и изъятия цифровых следов преступной деятельности.

Ключевые слова: сбыт наркотиков, «тайники-закладки», оперативный сотрудник, оперативно значимая информация, наркосбытчик, сеть Интернет, информационные технологии, электронные носители информации, киберпреступность, психотропные вещества.

Для цитирования:

Хамидуллин Р. С. Криминалистическое обеспечение противодействия незаконному обороту наркотических средств и психотропных веществ, осуществляемому в криптовалюте с использованием технологий «blockchain» // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 52–58.

Развитие современных технологий привело к проблемам выявления и раскрытия преступлений, связанных с незаконным оборотом наркотических средств и психотропных веществ. Покупатели и продавцы наркотиков получили

возможность заключать сделки и производить расчеты в сети Интернет, не осуществляя личных встреч, более того не зная друг друга. У правоохранительных органов возникли сложности в установлении связей между продавцом и

покупателем, а также установлении их «настоящих» данных. Современные возможности сети Интернет обеспечивают анонимность субъектов наркоторговли. Сами же наркотические средства из рук в руки напрямую не передаются, личная встреча отсутствуют, что возможно с помощью создания «тайников-закладок». В случае бесконтактного способа сбыта наркотиков, задержание самого сбытчика (закладчика, кладмена) или потребителя на месте нахождения «клада» (тайника с наркотиками) часто не позволяет установить всех участников преступной схемы ввиду всеобщей анонимности.

Сложность борьбы с наркоторговлей в сети Интернет заключается в использовании злоумышленниками его теневого сегмента – «DarkNet», который не контролируется ни одним государством. Данная сеть позволяет осуществлять оборот множества запрещенных предметов, включая поддельные денежные знаки (билеты) и даже оружие. Используя ресурсы площадки, наркопроизводители и наркоторговцы создают онлайн магазины (наркомаркеты), осуществляющие автоматический прием заявок на приобретение запрещенных психоактивных средств или химических веществ, а также

прекурсоров, которые используются при изготовлении различных наркотиков¹.

Наркоторговцам нужны были транзакции, которые сложно было бы отследить, такую возможность представили криптовалюты. Так появилась связь наркопреступности с оборотом криптовалюты, используемой для взаимных расчетов, а также легализации денежных средств, полученных преступным путем. Транзакции (операции с денежными средствами: перевод, вывод или зачисление на счет, т. е. любой процесс, связанный с использованием банковских счетов) в криптовалюте совершаются мгновенно и не имеют ограничений по территориальности, осуществляются по всему миру. При этом отсутствует единый эмиссионный центр и вне системы *SWIFT*, осуществляющей контроль за финансовыми и расчетными рисками относительно крупного характера совершаемых платежей при расчете за крупные партии наркотических средств².

Также стимулом выступает фиксированная, небольшая комиссия за совершение транзакций. Вместе с тем, одной из особенностей является анонимность в форме обезличенных криптосчетов в распределенном реестре финансовых операций, не позволяющих устанавливать

¹ Алиев Т. Ф., Столбова Н. А. Проблемы расследования преступлений, совершенных с использованием информационно-телекоммуникационной сети интернет // Научный дайджест Восточно-Сибирского института МВД России. 2021. № 4 (14). С. 12–17.

² Поздняков А. Н., Фирсова Е. В. Борьба с электронной наркокоммерцией – фрагменты реальности и перспектив: оперативно-розыскной аспект // Академическая мысль. 2020. № 3 (12). С. 23–32.

достаточные сведения для идентификации участников транзакций и бенефициаров криптовалютных средств. Обеспечивается данная техническая возможность в результате использования технологий Blockchain (выстроенная по определенным правилам непрерывная последовательная цепочка блоков (связанный список), содержащих информацию).

Таким образом, полученный доход не представляется возможным отследить. Цифровизация с помощью криптотехнологий лишает правоохранителя физического и юридического контроля за нелегальным наркооборотом и финансовыми операциями, проводимыми с ними.

Учитывая сложную и теневую систему преступных схем, связанных с децентрализованными и конвертируемыми видами управления виртуальными активами, в которых используются методы криптографии, для проверки и доказывания операций возникают новые сложные задачи, решить которые необходимо правоохранительным органам.

С этой целью оперативные сотрудники могут провести мониторинг обезличенных переводов криптовалюты, используя сервисы наподобие *blockchain.info*. Алгоритм при этом состоит из посещения главной страницы ресурса (*blockchain.info*) с последующим вводом кодов релевантной транзакции

криптовалюты. Таким образом, имеется возможность получить необходимую информацию и данные о состоянии сделки³.

Большинство сервисов при помощи алгоритмов могут сгенерировать уникальные адреса расчета с криптовалютами, при этом на разных сервисах могут использоваться одни и те же последовательности символов. Однако в Blockchain данный адрес попадает только после пополнения счета в криптовалюте. При анализе виртуальных транзакций может использоваться специальное сетевое приложение.

Существует перечень приложений – систем поиска виртуальных активов (например, Blockchain Explorer), которые на бесплатной основе предоставляют данные о переводах средств, связях между адресами криптокошельков. Такие данные могут помочь в своевременном корректировании направления работы, составлении аналитических связей при раскрытии и расследовании преступлений, в том числе связанных с незаконным оборотом наркотиков.

Дополнительным фактором анонимности выступают непубличные платформы с цифровыми активами. Отслеживание таких адресов будет затруднено. В частности, отдельные виды виртуальных активов – криптовалюты или «приватные монеты» (*privacycoins*), представляющие собой децентрализованное пиринговое

³ Исаков Р. В., Демко Н. М. Противодействие наркопреступности на примере организации разведывательной работы управления по борьбе с наркотиками (drug enforcement

administration) // Вестник Рязанского филиала Московского университета МВД России. 2020. № 14. С. 20–24.

сетевое средство стоимости или обмена, обеспечивают анонимность клиентов.

Для приобретения наркотических средств покупателю необходимо зарегистрироваться на каком-либо «обменнике» цифровых валют в сети Интернет, где у него будет находиться цифровой кошелек с уникальным адресом. Выглядеть адрес будет примерно так: 38AwYdyrG8yesfNjFKEQETaNu9nP Wtws. После чего покупателю необходимо приобрести криптовалюту (наиболее распространен Bitcoin) на сайте «обменника», для чего он выбирает предложение по приобретению определенного количества криптовалюты, где прямо на сайте «обменника» заключается сделка купли-продажи криптовалюты. «Обменник» выступает в роли третьей стороны, гаранта сделки (используется смарт-контракт), за что взимает соответствующую комиссию. Покупателю присылается номер банковской карты, на которую ему необходимо перевести эквивалентные количеству приобретаемой криптовалюты денежные средства. После подтверждения продавцом криптовалюты получения фиатных (это денежные средства, эмитированные (выпускаемые) государством, которые в настоящий момент времени являются законным платежным средством) денежных средств, «обменник» разблокирует с кошелька продавца криптовалюты то количество криптовалюты, которое приобреталось. Данный способ обмена поддается отслеживанию при помощи направления запросов в адрес

«обменника» и дальнейшей аналитической работы по установлению конкретных банковских счетов при взаимодействии с Росфинмониторингом. После чего проводятся мероприятия по установлению конкретных лиц – получателей денежных средств.

В ходе проведенного исследования нами выявлены некоторые сложности в раскрытии преступлений, совершаемых путем формирования «тайников-закладок» с наркотическими средствами. Имеющиеся схемы работы с технологиями конвертации криптовалюты все чаще становятся нерезультативными в связи с использованием интернет-площадок внутренних «обменников», цифровые кошельки которых формируются внутри интернет-площадки, и кошельков для хранения и передачи криптовалюты внутри сайта. Например, интернет-площадка «Hydra» использует указанные возможности постоянно, пополняя их новыми способами сокрытия данных своих ресурсов. Так, пользователь может выбрать различные способы оплаты, такие как:

1. Перевод денежных средств на банковскую карту. В данном случае сайт автоматически предоставляет номер банковской карты своего внутреннего «обменника» криптовалюты. Отслеживание денежных средств будет затруднено начиная с конвертации денежных средств и помещения их на цифровой кошелек, установить уникальный адрес которого не всегда представляется возможным.

2. Перевод по номеру телефона.

В данном случае оплата может производиться как с помощью онлайн-перевода для пополнения счета абонентского номера, так и с использованием «Qiwi-кошелек». Используемые сбытчиками абонентские номера, как правило, не имеют принадлежности, либо данные регистрации являются ложными. Для телефонной связи указанные номера не используются и чаще всего указываются однократно. В отношении «Qiwi-кошельков» схема установления участников преступной деятельности заключается в аналитической работе по результатам информации, полученной из запросов в «Qiwi-банк». При помощи подобной информации имеется возможность установить конечный абонентский номер или лицевой счет, используемый для вывода денежных средств. В связи с результативностью работы правоохранительных органов в данном направлении, использование «Qiwi-кошельков» сбытчиками значительно сократилось в их преступной деятельности.

3. Оплата при помощи криптовалюты, имеющейся на внутреннем кошельке сайта. Установление адресатов данного способа расчетов также затруднено в связи с минимальным временным промежутком между пополнением данного хранилища и оформления преступной сделки⁴.

Говоря о криминалистическом обеспечении противодействия незаконному обороту наркотических средств и психотропных веществ, осуществляемому в криптовалюте с использованием технологий «blockchain», необходимо отметить, что это комплекс мер направленных на получение оперативно значимой информации об обстоятельствах наркоторговли, а также особенности обнаружения, фиксация и процессуального оформления следов преступной деятельности в особенности их цифрового вида.

Необходимо помнить и о традиционных следах, так, при задержании лица подозреваемого в сбыте наркотиков необходимо незамедлительно получить следующие образцы для сравнительного исследования:

1) Букальный эпителий – для проведения биологической экспертизы и установления наличия ДНК на упаковке наркотического средства и иных предметах, имеющих значение для доказывания, а также для внесения ДНК задержанного в базу данных.

2) Смывы с обеих рук и срезы ногтевых пластин – для обнаружения на них частиц запрещенных веществ.

Кроме того, при задержании обязательными процедурами являются: фотографирование подозреваемого с постановкой на фотоучет; фотографирование подошвы обуви задержанного – для дополнительного доказывания путем

⁴ Хамидуллин Р. С. Обеспечение национальной безопасности путем противодействия преступлениям, связанным с незаконным оборотом наркотических средств и психотропных веществ,

совершаемым с использованием информационно-телекоммуникационных технологий // Вестник Уральского юридического института МВД России. 2022. № 1 (33). С. 93–98.

проведения сравнительных трасологических экспертиз и формирования базы данных; дактилоскопирование лица – для дополнительного доказывания путем проведения сравнительных экспертиз и внесения сведений в базу данных «Папилон».

В специализированных оперативно-розыскных подразделениях, таких как подразделения наркоконтроля МВД России имеются отделы, специализирующиеся на противодействии наркопреступности в сети Интернет с помощью производства оперативно-технических розыскных мероприятий. Кроме того, соответствующие подразделения Бюро специальных технических подразделений осуществляют первичное выявление цифровых

следов для их последующего оформления в ходе следственных действий и производства компьютерных экспертиз.

Таким образом, криминалистическое обеспечение противодействия незаконному обороту наркотических средств и психотропных веществ, осуществляемому в криптовалюте с использованием технологий «blockchain», представляет собой комплекс мер, направленных на обеспечение субъектов уголовного преследования знаниями о закономерностях наркооборота в сети Интернет и наиболее эффективных и рациональных криминалистических средствах, приемах и методах обнаружения, фиксации и изъятия следов в особенности их цифровых видов⁵.

Список литературы

1. Алиев Т. Ф. Проблемы расследования преступлений, совершенных с использованием информационно-телекоммуникационной сети интернет / Т. Ф. Алиев, Н. А. Столбова // Научный дайджест Восточно-Сибирского института МВД России. 2021. № 4 (14). С. 12–17.

2. Поздняков А. Н. Борьба с электронной наркокоммерцией – фрагменты реальности и перспектив: оперативно-розыскной аспект / А. Н. Поздняков, Е. В. Фирсова // Академическая мысль. 2020. № 3 (12). С. 23–32.

3. Исаков Р. В. Противодействие наркопреступности на примере организации разведывательной работы управления по борьбе с наркотиками (drug enforcement administration) / Р. В. Исаков, Н. М. Демко // Вестник Рязанского филиала Московского университета МВД России. 2020. № 14. С. 20–24.

4. Хамидуллин Р. С. Обеспечение национальной безопасности путем противодействия преступлениям, связанным с незаконным оборотом наркотических средств и психотропных веществ, совершаемым с использованием

⁵ Хамидуллин Р. С. Криминалистическое обеспечение деятельности следователя по применению норм особого порядка уголовного судопроизводства при

заключении досудебного соглашения о сотрудничестве: автореф. дис. ... канд. юрид. наук. Екатеринбург, 2018. 27 с.

информационно-телекоммуникационных технологий // Вестник Уральского юридического института МВД России. 2022. № 1 (33). С. 93–98.

5. Хамидуллин Р. С. Криминалистическое обеспечение деятельности следователя по применению норм особого порядка уголовного судопроизводства при заключении досудебного соглашения о сотрудничестве: автореф. дис. ... канд. юрид. наук. Екатеринбург, 2018. 27 с.

Ruslan S. Khamidullin

PhD (Law),

Head of the Department of Operative-Search Activities
Ural Law Institute of the Ministry of Internal Affairs of Russia
(Yekaterinburg, Russian Federation)
Rkhamidullin30@mvd.ru

FORENSIC SUPPORT OF COUNTERACTION TO ILLEGAL TRAFFICKING IN NARCOTIC DRUGS AND PSYCHOTROPIC SUBSTANCES CARRIED OUT IN CRYPTOCURRENCY USING BLOCKCHAIN TECHNOLOGIES

Abstract: This article discusses the problems of identifying, disclosing and investigating crimes in the field of drug trafficking carried out in cryptocurrency using blockchain technologies. An analysis was made of some features of using the shadow segment of the Internet "DarkNet" for the purpose of drug trafficking. In the study, special attention is paid to the forensic support of countering the trafficking of narcotic drugs committed by remote and non-contact means. Methods and techniques for identifying, fixing and seizing digital traces of criminal activity are proposed.

Keywords: drug sales, "caches", operational officer, operationally significant information, drug trafficker, Internet, information technology, electronic media, cybercrime, psychotropic substances.

УДК 340

Довгань Ксения Евгеньевна
Кандидат юридических наук,
доцент юридического института,
Алтайский государственный университет
(г. Барнаул, Российская Федерация)
dok2122@bk.ru

РАМОЧНОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация: Правовое регулирование в области информационных технологий носит рамочный характер. Отсутствие единого и комплексного правового акта создаёт трудности в области эффективного правового регулирования данных правоотношений. Использование рамочного регулирования законодателем обосновано ввиду неопределённости урегулирования всех аспектов развития информационных технологий. В связи с чем выбор оптимальных приёмов и способов правового регулирования и их последующая конкретизация представляется разумной и необходимой.

Ключевые слова: искусственный интеллект, рамочное законодательство, информационные технологии, правоотношение, правовое регулирование, национальные проекты.

Для цитирования:

Довгань К. Е. Рамочное регулирование информационных технологий в Российской Федерации // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 59–64.

В XXI веке информационные технологии (далее – ИТ) в различных аспектах существования стали объектом пристального исследования: фундаментальные вопросы изменения государства и права под влиянием цифрового, научно-технического, технологического вектора его

развития¹ стали объектом изучения учёных-юристов.

М. В. Залоило рассматривал подходы к определению и перспективы применения искусственного интеллекта², И. П. Кожокар выявлял недостатки нормативно-правового регулирования на судебное правоприменение в эпоху

¹ Концепция цифрового государства и цифровой правовой среды / Н. Н. Черногор, Д. А. Пашенцев, М. В. Залоило [и др.]. Москва, 2021. 244 с.

² Залоило М. В. Искусственный интеллект в праве: научно-практическое пособие. Москва, 2021. 132 с.

цифровизации права³, Н. Ш. Козаев изучал проблемы уголовного права в свете научного технического прогресса⁴, И. М. Рассолов исследовал право в кибернетическом пространстве⁵, А. Ю. Сафронов анализировал применение информационных технологий в уголовном судопроизводстве⁶, И. И. Шереметьев характеризовал дистанционный режим судебных заседаний⁷, Л. Ю. Василевская рассматривала токен как объект гражданских прав⁸, М. А. Егорова и О. В. Кожевина анализировали правовое регулирование криптовалюты⁹, В. С. Белых исследовал перспективные направления предпринимательского права в свете развития цифровой экономики¹⁰ и т. д.

Нам представляется важным рассмотрение технико-юридического аспекта закрепления правоотношений в области информационных технологий с точки зрения теории правового регулирования. Отсутствие единства в законодательном

закреплении развития цифровой экономики, правовых режимов информации, использование баз данных, защиты персональных данных и в других смежных вопросах создают трудности в осуществлении эффективного правового регулирования.

Нормативное правовое регулирование в области информационных технологий осуществляется на различных уровнях. Анализ современного законодательства показал устойчивое применение рамочного способа.

При этом в зарубежных странах отдают предпочтение законам для нормативного регулирования цифровой экономики и смежных вопросов в области информационных технологий. Например, в Великобритании существует Закон «О цифровой экономике» (Digital Economy act of 2017), который определяет цели и задачи регулирования цифровой экономики, а также указывает на необходимость рамочного регулирования отдельных

³ Кожокар И. П. Влияние недостатков нормативно-правового регулирования на судебное правоприменение в эпоху цифровизации права // Юридическая наука. 2019. № 7. С. 9–12.

⁴ Козаев Н. Ш. Современные проблемы уголовного права, обусловленные научно-техническим прогрессом. Москва, 2019. 480 с.

⁵ Рассолов И. М. Право и кибернетическое пространство. Монография (2-е издание). Москва, 2016. 232 с.

⁶ Сафронов А. Ю. Использование информационных технологий в суде по уголовным делам // Lex russica. 2022. № 3 (184). С. 105–118.

⁷ Шереметьев И. И. Использование современных цифровых технологий при

судебном разбирательстве уголовных дел в дистанционном режиме // Вестник Университета имени О. Е. Кутафина (МГЮА). 2020. № 10 (74). С. 97–107.

⁸ Василевская Л. Ю. Токен как новый объект гражданских прав: проблемы юридической квалификации цифрового права // Актуальные проблемы российского права. 2019. № 5 (102). С. 111–119.

⁹ Егорова М. А., Кожевина О. В. Место криптовалюты в системе объектов гражданских прав // Актуальные проблемы российского права. 2020. Т. 15, № 1 (110). С. 81–91.

¹⁰ Белых В. С. Цифровая экономика и развитие предпринимательского законодательства России // Бизнес, менеджмент и право. 2021. № 1 (49). С. 9–12.

вопросов. Последнее активно применяется в РФ – существует ряд соответствующих документов, действующих в сфере информационных технологий. Рассмотрим некоторые из них.

1. Национальные проекты, национальные программы.

Н. С. Кутузова при определении основных признаков и юридических свойств национального проекта как формы права отмечает его рамочный характер, соответствующие содержание и предписания¹¹. В качестве примера она рассматривает Федеральный проект «Нормативное регулирование цифровой среды» (п. 1.14), где «рамочность» проявляется в правовом требовании относительно издания сопутствующих нормативных актов: не определены название и конкретные особенности их содержания, а указывается только количество и окончательная дата принятия. В связи с такой неопределённостью национальных программ, национальных проектов возникает необходимость дальнейшей конкретизации их положений в иных актах.

2. Федеральные законы.

Среди федерального законодательства, регламентирующего вопросы правового регулирования ИТ стоит отметить федеральные законы о бюджете на соответствующих год, предполагающие финансирование

национальной программы «Цифровая экономика Российской Федерации». Их конкретизация проводится в рамках актов органов исполнительной власти.

Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона “О персональных данных”» от 24.04.2020 № 123-ФЗ в том числе предполагает конкретизацию отдельных положений по разработке и внедрению технологий искусственного интеллекта в законодательстве города федерального значения Москвы.

3. Указы Президента РФ.

В Послании Президента РФ В. В. Путина Федеральному Собранию РФ от 1 декабря 2016 г. сказано «запустить масштабную системную программу развития экономики нового технологического поколения, так называемой цифровой экономики. В её реализации будем опираться именно на российские компании, научные, исследовательские и инжиниринговые центры страны»¹². В этой связи были приняты соответствующие подзаконные акты, конкретизирующие Послание.

¹¹ Кутузова Н. С. Сущность и правовые аспекты национального проекта // Вестник Южно-Уральского государственного университета. Серия: Право. 2021. Т. 21, № 1. С. 96–102.

¹² Послание Президента РФ В. В. Путина Федеральному Собранию РФ от 1 декабря

2016 г. Текст послания официально опубликован не был // СПС «Консультант плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_207978/ (дата обращения: 10.05.2022).

Указ Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» (с изменениями и дополнениями) в пп. «б» п. 2 обозначил основу для разработки национальных проектов (программ) по серии направлений, в том числе цифровой экономики¹³.

Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» содержит раздел, посвящённый обеспечению национальных интересов в области цифровой экономики, в том числе «развития российской экосистемы цифровой экономики», «защита интересов российских граждан, обеспечение их занятости (развитие цифровой экономики не должно ущемлять интересы граждан)»¹⁴.

4. Акты Правительства РФ и иные подзаконные акты.

Правительством РФ в области развития ИТ был принят ряд актов. К

примеру, Постановление Правительства РФ от 2 марта 2019 г. № 234 «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации»¹⁵; Распоряжение Правительства РФ от 17.12.2019 № 3074-р «Концепция создания цифровой аналитической платформы» (вместе с «Концепцией создания цифровой аналитической платформы предоставления статистических данных») ¹⁶; Распоряжение Правительства РФ от 03.06.2019 № 1189-р «Об утверждении Концепции создания и функционирования национальной системы управления данными и плана мероприятий («дорожную карту») по созданию национальной системы управления данными на 2019–2021 годы»¹⁷; Постановление Правительства РФ от 14.05.2021 № 733 «Об утверждении Положения о федеральной государственной информационной системе «Единая информационная платформа национальной системы управления данными» и о внесении

¹³ О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года (с изменениями и дополнениями): указ Президента РФ от 7 мая 2018 г. № 204 // Собрание законодательства Российской Федерации. 2018. № 20. Ст. 2817.

¹⁴ О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указ Президента РФ от 9 мая 2017 г. № 203 // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

¹⁵ О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации»: постановление Правительства РФ от 2 марта 2019 г. № 234 (с изменениями и дополнениями) // Собрание законодательства Российской Федерации. 2019. № 11. Ст. 1119.

¹⁶ Концепция создания цифровой аналитической платформы (вместе с «Концепцией создания цифровой аналитической платформы предоставления статистических данных»): распоряжение Правительства РФ от 17 декабря 2019 № 3074-р // Собрание законодательства РФ. 2019. № 52 (часть II). Ст. 8054.

¹⁷ Об утверждении Концепции создания и функционирования национальной системы управления данными и плана мероприятий («дорожную карту») по созданию национальной системы управления данными на 2019–2021 годы: распоряжение Правительства РФ от 3 июня 2019 № 1189-р // Собрание законодательства РФ. 2019. № 23. Ст. 3041.

изменений в некоторые акты Правительства Российской Федерации»¹⁸ и многие другие.

Согласно вышеописанному принципу, акты Правительства РФ, созданные в рамках рамочного регулирования, включают относительно определённые нормы, требующие дополнительной конкретизации на уровне органов исполнительной власти РФ либо субъектов РФ.

Анализ законодательства позволяет выявить определённую тенденцию, а именно, использование законодателем рамочного правового регулирования с целью дальнейшей конкретизации, что позволяет достичь необходимого уровня конкретизации и создать правовую базу для дальнейшего нормативного правового регулирования новых правоотношений в области ИТ.

Список литературы

1. Белых В. С. Цифровая экономика и развитие предпринимательского законодательства России // Бизнес, менеджмент и право. 2021. № 1 (49). С. 9–12.
2. Василевская Л. Ю. Токен как новый объект гражданских прав: проблемы юридической квалификации цифрового права // Актуальные проблемы российского права. 2019. № 5 (102). С. 111–119.
3. Егорова М. А. Место криптовалюты в системе объектов гражданских прав / М. А. Егорова, О. В. Кожевина // Актуальные проблемы российского права. 2020. Т. 15, № 1 (110). С. 81–91.
4. Залоило М. В. Искусственный интеллект в праве: научно-практическое пособие. Москва, 2021. 132 с.
5. Кожокаръ И. П. Влияние недостатков нормативно-правового регулирования на судебное правоприменение в эпоху цифровизации права // Юридическая наука. 2019. № 7. С. 9–12.
6. Козаев Н. Ш. Современные проблемы уголовного права, обусловленные научно-техническим прогрессом. Москва, 2019. 480 с.
7. Концепция цифрового государства и цифровой правовой среды / Н. Н. Черногор, Д. А. Пашенцев, М. В. Залоило [и др.]. Москва, 2021. 244 с.
8. Кутузова Н. С. Сущность и правовые аспекты национального проекта // Вестник Южно-Уральского государственного университета. Серия: Право. 2021. Т. 21, № 1. С. 96–102.
9. Рассолов И. М. Право и кибернетическое пространство. Монография (2-е издание). Москва, 2016. 232 с.
10. Сафронов А. Ю. Использование информационных технологий в суде по уголовным делам // Lex russica. 2022. № 3 (184). С. 105–118.

¹⁸ Об утверждении Положения о федеральной государственной информационной системе «Единая информационная платформа национальной системы управления данными» и о внесении изменений в

некоторые акты Правительства Российской Федерации: постановление Правительства РФ от 14 мая 2021 № 733 // Собрание законодательства РФ. 2021. № 21. Ст. 3585.

11. Шереметьев И. И. Использование современных цифровых технологий при судебном разбирательстве уголовных дел в дистанционном режиме // Вестник Университета имени О. Е. Кутафина (МГЮА). 2020. № 10 (74). С. 97–107.

Ksenia E. Dovgan

PhD (Law), Associate Professor of the Law Institute,
Altai State University
(Barnaul, Russian Federation)
dok2122@bk.ru

FRAMEWORK REGULATION OF INFORMATION TECHNOLOGIES IN THE RUSSIAN FEDERATION

Abstract: Legal regulation in the field of information technology is of a framework nature. The absence of a single and comprehensive legal act creates difficulties in the field of effective legal regulation of these legal relations. The use of framework regulation by the legislator is justified due to the uncertainty of the settlement of all aspects of the development of information technologies. In this connection, the choice of the optimal methods and methods of legal regulation and their subsequent specification seems reasonable and necessary.

Keywords: artificial intelligence, framework legislation, information technology, legal relationship, legal regulation, national projects.

УДК 343.98

Долинин Владимир Николаевич

Кандидат юридических наук, доцент,
доцент кафедры криминалистики,

Уральский государственный юридический университет
имени В. Ф. Яковлева
(Екатеринбург, Российская Федерация)
dvn1952@gmail.com

Пермяков Евгений Константинович

Студент,

Уральский государственный юридический университет
имени В. Ф. Яковлева
(Екатеринбург, Российская Федерация)
zhen.permyakov@yandex.ru

Ровнушкин Вадим Евгеньевич

Студент,

Уральский государственный юридический университет
имени В. Ф. Яковлева
(Екатеринбург, Российская Федерация)
rve20000@mail.ru

ИСПОЛЬЗОВАНИЕ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация: В представленной статье приводятся некоторые определения информационных технологий, предложенных различными авторами, а также законодателем. Рассматривается содержание информационных процессов и их структура. Описаны классификации информационных технологий и позиции учёных по этому вопросу. Авторы подчёркивают, что в настоящее время информационные технологии нашли широкое применение в сфере юриспруденции, поскольку способствуют быстрому поиску, переработке и анализу конкретной информации. Большое внимание уделено вопросам использования компьютерных технологий в правоохранительной деятельности. В статье приведены и описаны некоторые автоматизированные информационно-поисковые системы. Авторы убеждены, что АИПС значительно облегчает работу сотрудников правопорядка и способствуют более успешному раскрытию и расследованию преступлений.

Ключевые слова: информационные технологии, использование, правоохранительная деятельность, геномная информация, автоматизированные информационные системы.

Для цитирования:

Долинин В. Н., Пермяков Е. К., Ровнушкин В. Е. Использование компьютерных технологий в правоохранительной деятельности // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 65–75.

Информационные технологии начали развиваться с двадцать первого века. Их применение можно повстречать буквально везде, в каждой сфере общечеловеческого бытия. На сегодняшний день, любой человек, будь то школьник или специалист в сфере кибербезопасности, пользуется компьютером, планшетом, смартфоном и рядом других гаджетов для выполнения определённых ежедневных задач. Но при этом до сих пор нет строгого и чёткого определения понятия «информационные технологии», можно встретить разные трактовки¹. Однако многие учёные и специалисты сегодня считают верной следующую: информационные технологии – это технологии, которые базируются на новейшей компьютерной технике. Так, В. Д. Элькин информационную технологию определяет, как «совокупность процессов, методов поиска, сбора, хранения, обработки, предоставления, распространения информации и способов осуществления таких процессов и методов»²

Законодатель под «информационными технологиями» понимает процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов, а под «информацией» – сведения (сообщения, данные) независимо от формы их представления³.

Из приведённых выше определений видно, что информационные технологии включают в себе систему процессов:

1) «Сбор информации – это деятельность субъекта, в ходе которой он получает сведения об интересующем его объекте.

2) Обмен информацией – это процесс, в ходе которого источник информации ее передает, а получатель – принимает.

3) Хранение информации – это процесс поддержания исходной информации в виде, обеспечивающем выдачу данных по запросам конечных пользователей в установленные сроки.

¹ Хлебников А. А. Информационные технологии: учебник М., 2016. С. 40.

² Элькин В. Д. Информационные технологии в юридической деятельности. Учебник и практикум для вузов. 2-е изд., пер. и доп., М, 2018. С. 22.

³ Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 30.12.2021) «Об информации,

информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.01.2022) // СПС «КонсультантПлюс». URL:

http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 10.05.2022). Пункт 1, 2 ст. 2.

4) Обработка информации – преобразование информации из одного вида в другой»⁴.

5) «Кроме того, полученную информацию необходимо использовать в практической деятельности»⁵.

В настоящее время существуют различные классификации информационных технологий. Так, К. Х. Калугян предложил следующую:

- «по типу обрабатываемой информации;
- по форме реализации;
- по типу пользовательского интерфейса;
- по способу использования программ;
- по способу обработки информации»⁶.

Ю. Ю. Громов классифицировал информационные технологии:

- по признаку сферы применения;
- по назначению и характеру использования;
- по пользовательскому интерфейсу;
- по способу организации сетевого взаимодействия;
- по принципу построения;
- по степени охвата задач управления;

- по характеру участия технических средств в диалоге с пользователем;

- по способу управления производственной технологией»⁷.

По нашему мнению, указанные выше классификации являются неполными, к ним следует добавить основание «по области деятельности». Оно включает в себя такие сферы, как:

- медицина,
- банковская деятельность,
- страховая деятельность,
- юридическая деятельность,
- судебная деятельность,
- правоохранительная деятельность и многие другие.

В настоящее время информационные технологии нашли широкое применение в сфере юриспруденции, где дают возможность разрешить широкий круг проблем, возникающих при выполнении юристами своих должностных обязанностей. Применение данных технологий обобщило весь массив информации по определённым темам, разделам, группам, что значительно позволило сократить время поиска требуемых сведений. Помимо этого, информационные технологии позволяют не только извлекать необходимой информацию из баз данных, но и изменять её, а также

⁴ Хлебников А. А. Информационные технологии: учебник. М.: КНОРУС, 2016. С. 37–39.

⁵ Советов Б. Я., Цехановский В. В. Информационные технологии: учебник. 6-е изд., перераб. и доп. М.: Издательство Юрайт, 2015. С. 44.

⁶ Калугян К. Х. Информационные технологии: учебное пособие. Ростов-на-

Дону: Издательско-полиграфический комплекс Рост. гос. экон. ун-та (РИНХ), 2020. С. 54–55.

⁷ Информационные технологии: учебник / Ю. Ю. Громов, И. В. Дидрих, О. Г. Иванова [и др.]. Тамбов: Изд-во ФГБОУ ВПО «ТГТУ», 2015. С. 41–56.

обмениваться ею между абонентами. Так, например, сотрудники правоохранительных органов могут с лёгкостью узнавать аналитические и статистические данные, которые требуются для разрешения их проблем. Адвокаты же могут находить судебные решения по аналогичным делам, извлекать для себя определённую информацию и использовать её в дальнейшем для построения линии защиты в суде. Самой «главной и самой ценной наработкой информационной технологии, которая существенно облегчила работу любого юриста, стало появление справочно-правовой системы»⁸.

Предпосылкой её появления стало скопление большого объёма бумажной информации к началу семидесятых годов двадцатого века. Со временем этот массив только увеличивался. Однако параллельно шло развитие информационных технологий, что позволило органам государственной власти, юристам и другим заинтересованным лицам обратиться к специалистам в данной области для создания в соответствии с профессиональными запросами определённых справочно-правовых систем, а в дальнейшем – и их мобильных версий. Например, «КонсультантПлюс» – крупнейший правовой информационный ресурс, содержащий свыше 256 000 000 документов федерального и регионального законодательства, а

также судебных решений, финансовых консультаций, комментариев к законодательству и других полезных материалов.

Информация, включённая в систему, структурирована по следующим разделам:

- законодательство;
- судебная практика;
- финансовые и кадровые консультации;
- консультации для бюджетных организаций;
- комментарии законодательства;
- формы документов;
- законопроекты;
- международные правовые акты;
- правовые акты по здравоохранению;
- технические нормы и правила.

«В основе КонсультантПлюс лежат современные программные технологии, которые постоянно совершенствуются – каждый год в системе появляются новые возможности, которые облегчают работу и экономят время пользователей. Путеводители КонсультантПлюс помогают экономить время пользователей на самостоятельное изучение информации по сложным вопросам»⁹. Путеводители охватывают широкий круг практических вопросов, начиная сделками и заканчивая обзором

⁸ Шашин М. А. Информационные технологии в юридической деятельности URL: https://spravochnick.ru/informacionnye_tehnologii/informacionnye_tehnologii_v_yuridicheskoy_deyatelnosti/ (дата обращения: 10.05.2022).

⁹ Информационные технологии в юридической деятельности: учебное пособие / Т. М. Беляева [и др.]; под ред. В. Д. Элькина. Москва: Юрайт, 2012. С. 163–166.

судебной практики по ним. Также, материалы содержат выводы, определённые мнения специалистов, ссылки на сопутствующие документы и другую полезную информацию.

«В судебной деятельности используется ГАС «Правосудие». ГАС «Правосудие» – это территориально распределённая автоматизированная информационная система, предназначенная для формирования единого информационного пространства судов общей юрисдикции и системы Судебного департамента при Верховном Суде РФ»¹⁰. Данная система предназначена для распределения уголовных и гражданских дел. Кроме того, она способствует проведению судебных заседаний в формате видеоконференцсвязи при невозможности участника процесса присутствовать в зале лично, что значительно облегчает работу судебных работников.

Принцип работы данной системы прост. Рассмотрим на примере гражданского дела. Исковое заявление поступает в суд, секретарь которого регистрирует его в системе. После этого новому делу присваивается определённый индивидуальный номер и за ним закрепляется конкретный судья. Система учитывает количество дел, закреплённых за каждым судьёй, и выбирает того, у кого их меньше, по сравнению с коллегами. Таким образом нагрузка распределяется

равномерно, что оптимизирует деятельность судей.

Очередным этапом в развитии информационных технологий в юриспруденции стало появление автоматизированных информационных систем. Сегодня таковые с успехом используются в государственных организациях, делопроизводстве, и других видах деятельности. Например, есть автоматизированные информационные системы для применения в работе правоохранительных органов, с целью интеграции которых уже с 2005 года начали внедряться автоматизированные рабочие места. Это приблизило нас к созданию единой информационной и телекоммуникационной системы Министерства Внутренних Дел России.

«На базе ГИАЦ МВД России создана межведомственная автоматизированная система ведения Регистра Федерального интегрированного информационного фонда, предусматривающая интеграцию информационных ресурсов и информационное взаимодействие министерств и ведомств правоохранительных и судебных органов»¹¹.

В прокуратуре используется программа АРМ «Статистика», которая формирует статистическую информацию о деятельности органов прокуратуры всех уровней и является основой для проведения

¹⁰ Информационные технологии в юридической деятельности: учебник / П. У. Кузнецов [и др.]; под общ. ред. П. У. Кузнецова. 3-е изд., перераб. и доп. Москва: Издательство Юрайт, 2020. С. 272.

¹¹ Информационные технологии в юридической деятельности: учебник и практикум / В. Д. Элькин [и др.]; под ред. В. Д. Элькина. 2-е изд., перераб. и доп. Москва: Издательство Юрайт, 2022. С. 193.

аналитической работы. Во многих прокуратурах субъекта внедрена АИС «Кадры». В ней содержится информация о каждом сотруднике, в том числе его семейное положение, должность, звание, с какого года работает и многое другое.

Учётная информация имеет особое значение в системе МВД России, она помогает в раскрытии, расследовании и предупреждении преступлений, розыске преступников, установлении личности неизвестных граждан, принадлежности изъятого имущества и т. д. Такая информация формируется в городских и районных органах, ИЦ органов МВД России по территориальному (региональному) принципу и образует федеральные учёты ГИАЦ МВД России. «Проведенная работа по автоматизации и объединению в едином банке данных оперативно-справочных, розыскных, криминалистических и статистических учетов позволила создать систему, которая является мощным оружием в руках правоохранительных органов в борьбе с преступностью. Это позволяет объединить все эксплуатируемые автоматизированные системы для дальнейшего формирования единого информационного пространства всех правоохранительных органов»¹².

Централизованные оперативно-справочные, криминалистические и розыскные учёты располагают следующими сведениями о гражданах

России, иностранцах и лицах без гражданства:

- судимость, место и время отбывания наказания, дата и основание освобождения;
- перемещение осуждённых;
- смерть в местах лишения свободы, изменение приговора, амнистия, номер уголовного дела;
- место жительства и место работы до осуждения;
- задержание за бродяжничество.

«Учетная информация создается и обрабатывается в автоматизированных информационно-поисковых системах»¹³ (АИПС). Приведём краткую характеристику отдельных их видов:

АИПС «Картотека» – автоматизированный пофамильный и дактилоскопический учёт. Служит для получения сведений о судимости, местах жительства и работы до осуждения, группе крови, дактилоскопической формуле.

АИПС «Опознание» выдаёт информацию о лицах, пропавших без вести, неопознанных трупах, неизвестных больных и детях.

АИПС «Автопоиск» содержит информацию о легковых и грузовых автомобилях, автобусах отечественного и иностранного производства со следующими установочными данными: государственный номер, номера двигателя, кузова и шасси. В информационных центрах МВД,

¹² Информационные технологии в юридической деятельности: учебник / П. У. Кузнецов [и др.]; под общ. ред. П. У. Кузнецова. 3-е изд., перераб. и доп. Москва: Издательство Юрайт, 2020. С. 306.

¹³ Бурцева И. В., Селезнёв А. В., Чернышов В. Н. Информационные технологии в юриспруденции: учеб. пособие. Тамбов: Изд-во ФГБОУ ВПО «ТГТУ», 2012. С. 21.

УМВД дополнительно осуществляется регистрация мотоциклов, мотороллеров и мотоколясок.

«АИПС «Досье» позволяет получить сведения об особо опасных рецидивистах, «ворах в законе», «авторитетах» преступного мира и др.:

- установочные данные,
- приметы,
- место работы,
- место жительства,
- связи,
- привычки и т. д.

Сотрудники правоохранительных органов обращаются с письменным запросом к исполнителю и получают интересующую их информацию»¹⁴.

АДИС (автоматизированная дактилоскопическая идентификационная система) – программно-технический комплекс, предназначенный для ведения дактилоскопических учётов и осуществления проверок следов рук, изъятых с мест нераскрытых преступлений, по массивам дактилокарт лиц, состоящих на дактилоскопическом учёте.

За последние годы разработано и апробировано несколько АДИС, наиболее совершенной из которых признана система «Папилон», использующая самое полное топологическое описание гребневой структуры папиллярного узора и автоматический кодер высокой точности и надёжности, не требующий

участия оператора при кодировании узора. Эта система уже внедрена в большинстве регионов страны.

Данная система проста в эксплуатации и обеспечивает:

- ввод и хранение в базе данных дактилокарт, фотоизображений лиц, особых примет и словесного описания людей;
- ввод и хранение следов пальцев рук и ладоней, изъятых с мест нераскрытых преступлений;
- автоматический поиск «карта-карта» для установления личности проверяемого субъекта;
- автоматический поиск «карта-след» и «след-карта» для выявления лица, оставившего следы пальцев на месте происшествия либо нескольких таких местах;
- автоматический поиск «след-след», чтобы установить факт совершения нескольких преступлений одним и тем же человеком, на момент проверки неизвестным;
- поиск и идентификацию следов и отпечатков ладоней;
- автоматизированное определение дактилоформулы;
- удалённый ввод дактилоскопической информации, удалённый доступ к центральной базе данных¹⁵.

Система АДИС «Папилон», «работающая в конкретном субъекте Российской Федерации, имеет центральную компьютерную систему и связанную с ней сеть станций

¹⁴ Драпкин Л. Я., Карагодин В. Н. Криминалистика: учебник. 2-е изд., перераб. и доп. Москва: Проспект, 2011. С. 157.

¹⁵ Криминалистика для следователей и дознавателей: научно-практическое пособие /

Е. П. Ищенко [и др.]; под общ. ред. А. В. Аничина; Московская гос. юридическая акад. им. О. Е. Кутафина. Москва: ИНФРА-М, 2009. С. 456–457.

удаленного доступа, охватывающих весь регион. В центральной АДИС, полностью аккумулирующей дактилоскопическую информацию, производятся все проверки и выдаются результаты. На станциях удаленного доступа вводится информация оперативного учета (дактилокарты, следы, словесные описания, фотографии), передаваемая в центр для выполнения проверок. Она сразу же вливается в базу данных и становится доступной всем другим удаленным пользователям. Дактилоскопирование преступников производится на «живом» сканере Папилон, являющемся уникальным оптоэлектронным устройством бесцветного дактилоскопирования. Он формирует изображение прокатанного пальца, контрольных отпечатков, отпечатков ладоней. Папиллярный узор фиксируется точно, возможна многократная прокатка для получения оптимального результата»¹⁶.

Порядок следования, расположение отпечатков и контрольных отпечатков регулируется автоматически. Получаемые таким образом электронные дактилокарты сжимаются и за считанные минуты передаются в любую другую АДИС.

В органах МВД РФ распространена система АБИС «Арсенал», её применение позволяет создавать электронные пулегильзотеки объемом в десятки и сотни тысяч объектов и выводит на качественно новый уровень выполнение баллистических экспертиз

выстрелянных пуль, их фрагментов и стреляных гильз при расследовании преступлений, связанных с применением огнестрельного оружия.

Создаваемые АБИС «Арсенал» электронные базы данных и современный уровень развития коммуникационных сетей открывают возможности для организации удалённого доступа к базам данных и межрегионального обмена информацией по огнестрельному оружию.

Принцип работы АБИС «Арсенал» предельно прост. Пуля или гильза погружается в специальный сканер, который считывает информацию с объекта, в частности, его рельеф. Сканирование происходит по всем осям. Далее информация выводится на экран компьютера в виде картинок и попадает в базу данных. На таких изображениях отчётливо видны царапины на боковых поверхностях пули или гильзы, их номера, следы удара бойка по капсюлю и многое другое.

Кроме того, органами правопорядка активно используется геномная информация. Соответствующая регистрация обязательна для:

- осуждённых и лиц, которые отбывают наказание в виде лишения свободы за совершение тяжких или особо тяжких преступлений;
- лиц, совершивших преступления против половой неприкосновенности и половой свободы личности;

¹⁶ Криминалистика: учебник / Т. В. Аверьянова [и др.]. 4-е изд., перераб. и доп. Москва: Норма: Инфра-М, 2013. С. 389.

- неустановленных лиц и неопознанных трупов.

Регистрация проводится:

- учреждениями, исполняющими уголовные наказания в виде лишения свободы в отношении лиц, которые были осуждены и отбывают наказания;

- органами предварительного следствия, органами дознания совместно с учреждениями судебно-медицинской экспертизы в отношении неустановленных лиц;

- органами предварительного следствия, органами дознания и органами, осуществляющими оперативно-розыскные мероприятия совместно с учреждениями судебно-медицинской экспертизы в отношении неопознанных трупов.

Государственная геномная регистрация осуществляется органами, учреждениями совместно с органами внутренних дел Российской Федерации¹⁷.

«Получение геномной информации при проведении государственной геномной регистрации осуществляется: путём получения образцов биологического материала у разных субъектов для проведения генетической экспертизы»¹⁸.

К целям использования геномной информации относятся:

1) предупреждение, раскрытие и расследование преступлений, а также

выявление и установление лиц, их совершивших;

2) розыск пропавших без вести граждан Российской Федерации, а также иностранных граждан и лиц без гражданства, проживающих или временно пребывающих на территории Российской Федерации;

3) установление личности человека, чей труп не опознан иными способами;

4) установление родственных отношений, разыскиваемых или устанавливаемых лиц.

Использовать геномную информацию имеют право суды, органы предварительного следствия, органы дознания и органы, осуществляющие оперативно-розыскную деятельность.

Принимая во внимание вышеизложенное, необходимо сделать следующие выводы:

1. Существующую классификацию информационных технологий предлагаем расширить по основанию «области деятельности». Это позволит повысить практическую значимость АИПС;

2. В настоящее время правоохранительная деятельность практически невозможна без применения АИПС, поскольку сотрудники органов правопорядка, обращаясь в АИПС, получают необходимую и конкретную информацию;

¹⁷ Ст. 7, 8 Федерального закона от 03.12.2008 № 242-ФЗ «О государственной геномной регистрации в Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_82263/ (дата обращения: 10.05.2022).

¹⁸ Криминалистика для следователей и дознавателей: научно-практическое пособие / Е. П. Ищенко [и др.]; под общ. ред. А. В. Аничина; Московская гос. юридическая акад. им. О. Е. Кутафина. Москва: ИНФРА-М, 2009. С. 217–218.

3. Использование компьютерных технологий не только облегчает деятельность правоохранительных органов, но и способствует более эффективному раскрытию и расследованию преступлений, особенно серийных, совершённых в условиях неочевидности;

4. Целесообразно разработать компьютерную программу расследования корыстно-насильственных серийных преступлений на основе изучения и обобщения большого массива уголовных дел данной категории с использованием искусственного интеллекта по типу системы «Маньяк».

Список литературы

1. Бурцева И. В. Информационные технологии в юриспруденции: учеб. пособие / Е. В. Бурцева, А. В. Селезнёв, В. Н. Чернышов. Тамбов: Изд-во ФГБОУ ВПО «ТГТУ», 2012. 104 с.
2. Драпкин Л. Я. Криминалистика: учебник / Л. Я. Драпкин, В. Н. Карагодин. 2-е изд., перераб. и доп. Москва: Проспект, 2011. 766 с.
3. Информационные технологии в юридической деятельности: учебник / П. У. Кузнецов [и др.]; под общ. ред. П. У. Кузнецова. 3-е изд., перераб. и доп. Москва: Издательство Юрайт, 2020. 325 с.
4. Информационные технологии в юридической деятельности: учебник и практикум / В. Д. Элькин [и др.]; под ред. В. Д. Элькина. 2-е изд., перераб. и доп. Москва: Издательство Юрайт, 2022. 472 с.
5. Информационные технологии в юридической деятельности: учебное пособие / Т. М. Беляева [и др.]; под ред. В. Д. Элькина. Москва: Юрайт, 2012. 352 с.
6. Информационные технологии: учебник / Ю. Ю. Громов, И. В. Дидрих, О. Г. Иванова [и др.]. Тамбов: Изд-во ФГБОУ ВПО «ТГТУ», 2015. 260 с.
7. Калугян К. Х. Информационные технологии: учебное пособие. Ростов-на-Дону: Издательско-полиграфический комплекс Рост. гос. экон. ун-та (РИНХ), 2020. 84 с.
8. Криминалистика для следователей и дознавателей: научно-практическое пособие / Е. П. Ищенко [и др.]; под общ. ред. А. В. Аничина; Московская гос. юридическая акад. им. О. Е. Кутафина. Москва: ИНФРА-М, 2009. 683 с.
9. Криминалистика. Полный курс: учебник для вузов / под общ. ред. А. Г. Филиппова. 5-е изд., перераб. и доп. М.: Издательство Юрайт, 2020. 855 с.
10. Криминалистика: учебник / Т. В. Аверьянова [и др.]. 4-е изд., перераб. и доп. Москва: Норма: Инфра-М, 2013. 927 с.
11. Советов Б. Я. Информационные технологии: учебник / Б. Я. Советов, В. В. Цехановский. 6-е изд., перераб. и доп. М.: Издательство Юрайт, 2015. 261 с.
12. Хлебников А. А. Информационные технологии: учебник. М.: КНОРУС, 2016. 466 с.

13. Чубукова С. Г. Основы правовой информатики (юридические и математические вопросы информатики): учебное пособие / С. Г. Чубукова, В. Д. Элькин; под ред. М. М. Рассолова. Изд. 2-е, испр. и доп. Москва: Контракт: ИНФРА-М, 2008. 276 с.

14. Шашин М. А. Информационные технологии в юридической деятельности URL: https://spravochnick.ru/informacionnye_tehnologii/informacionnye_tehnologii_v_yuridicheskoy_deyatelnosti/.

Vladimir N. Dolinin

PhD (Law), Associate Professor,
Associate Professor of the Department of Criminalistics,
Ural State Law University named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
dvn1952@gmail.com

Evgeny K. Permyakov

Student,
Ural State Law University named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
zhen.permyackov@yandex.ru

Vadim E. Ravnushkin

Student,
Ural State Law University named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
Rve20000@mail.ru

THE USE OF COMPUTER TECHNOLOGY IN LAW ENFORCEMENT

Abstract: The article presents some definitions of information technologies proposed by various authors, as well as the formulation of the legislator. The content of information processes and their structure are considered. The classifications of information technologies and the positions of scientists on this issue are described. The authors emphasize that currently information technologies have found wide application in the field of jurisprudence, as they contribute to the rapid search, processing and analysis of specific information. Much attention is paid to the use of computer technology in law enforcement. The article presents and describes some automated information retrieval systems. The authors are convinced that AIPS greatly facilitates the work of law enforcement officers and contributes to more successful detection and investigation of crimes.

Keywords: information technology, usage, law enforcement, genomic information, automated information systems.

Зазулин Анатолий Игоревич
Кандидат юридических наук,
Старший юрист юридической фирмы INTELLECT
(г. Екатеринбург, Российская Федерация)
a.zazulin@intellectmail.ru

AUTOMATION BIAS (ОШИБКА АВТОМАТИЗАЦИИ): ЕЩЁ ОДНА ПРОБЛЕМА ВНЕДРЕНИЯ ТЕХНОЛОГИЙ ИИ В ПРАВОСУДИИ

Аннотация: Статья посвящена мало изученной в российской юридической литературе теме взаимодействия человека и искусственного интеллекта в сфере принятия процессуальных решений. Во всё большем количестве стран реализуются попытки интегрировать новейшие технологии обработки больших данных в систему юстиции: разрабатываются ПО поддержки принятия судебных решений в части расчёта размера суммы залога или уголовного наказания. С целью исследования возможных рисков модели «ИИ – судья», автор провёл анализ того, как изменялись модели принятия судебных решений на пути развития уголовного процесса, а также какие факторы влияют на сознательный или неосознанный отход от принципа объективности. Одним из таких факторов является ошибка автоматизации (automation bias) – склонность человека принимать «на веру» рекомендации алгоритмов ИИ. В статье приведены возможные негативные правовые последствия игнорирования ошибки автоматизации при интеграции ИИ-технологий в правосудие.

Ключевые слова: искусственный интеллект, процессуальное решение, формальная теория доказательств, когнитивное искажение, ошибка автоматизации.

Для цитирования:

Зазулин А. И. Automation bias (ошибка автоматизации): ещё одна проблема внедрения технологий ИИ в правосудие // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 76–85.

Процесс принятия судьёй решения является ядром любого судопроизводства, в том числе уголовного. Именно там, за закрытыми дверями совещательной комнаты, творится «магия»: взвешиваются доводы защиты и обвинения, оцениваются все обстоятельства дела и доказательства, определяются

подлежащие применению правовые нормы, а также учитываются позиции и толкования вышестоящих судов. В этот момент с судьи «спадают» функции по руководству судебным заседанием, контролю соблюдения правил доказывания, разъяснению вопросов перед присяжными и их напутствию. Остаётся только одна

главная задача, заключающаяся, как писал С. С. Алексеев, в конечном правоприменительном действии, решении дела по существу¹.

Однако как именно происходит принятие судебного решения? Что творится в голове судьи во время этого процесса? Может ли быть обеспечена полная объективность и беспристрастность суда? Судья всегда был для остальных участников процесса и общества своеобразным «котом в мешке», «чёрной коробкой», и первоначальные механизмы уголовного судопроизводства (после его отделения от частного процесса и превращения в публичную отрасль права) были направлены на ограничение степени непредсказуемости судебного решения и произвола суда.

Так, формальная теория доказательств в своём роде полностью разрешала указанную проблему. Каждому доказательству присваивался свой вес и значение, а задача судьи заключалась в том, чтобы убедиться в наличии достаточного набора определённых законом доказательств. Это существенно упрощало процесс принятия итогового решения – от судьи не требовалось самостоятельного суждения. Как указывал В. Д. Спасович, «формальная теория доказательств ставит закон так, что подсудимый не зависит от произвола судьи, от его личного безотчетного впечатления. Но прямо

от закона судье оставалось только механически взвешивать доказательства объективно, законом данною меркою, и быть простым орудием и исполнителем закона, не принимая ничего на свою совесть»².

Обратной стороной медали являлось смещение фокуса от судейского суждения к самому доказыванию: вместо воздействия на судью применялись способы получения «совершенных» доказательств, таких как собственное признание подсудимого. Вопреки распространённому мнению, судьям было известно, что под пыткой могут быть даны любые показания. Между тем также считалось, что такой опасности можно избежать, если сделанное под пыткой признание будет повторено обвиняемым перед судьей без пыточного воздействия. Для этого, в частности, и велось протоколирование признаний обвиняемого – с целью их последующей сверки с показаниями подсудимого в судебном заседании³. Польза такого подхода, однако, нивелировалась тем, что в случае отрицания подсудимым своей вины перед судом его ждало повторение пыток – поэтому, казалось бы, добровольное признание вины на самом деле никак не гарантировало устранения риска самооговора⁴. Таким образом, формальная теория доказательств с одной стороны защищала от судейского произвола, а с

¹ Алексеев С. С. Общая теория права. М.: Проспект, 2010. С. 321.

² Спасович В. Д. О теории судебно-уголовных доказательств. В связи с судоустройством и судопроизводством. М.: ЛексЭст, 2001. С. 13

³ Niehaus M. Das Verhör. Geschichte – Theorie – Fiktion. München: Wilhelm Fink Verlag, 2003. S. 204.

⁴ Heghmanns M. Strafverfahren Strafrecht für alle Semester Grund- und Examenswissen kritisch vertieft. Springer, 2014. S. 14.

другой – поощряла произвол следственный.

Современная концепция принятия судебного решения основывается на принципе свободной оценки доказательств, придавая большое значение внутреннему убеждению судьи и не предопределяя за каким-либо видом доказательства заранее установленной доказательственной силы. Эта концепция берёт своё начало из идей гуманизма и рациональности, окончательно укрепившихся в западных обществах к середине XIX века.

Уголовный процесс, представляя собой идеальную модель судопроизводства, требует от судьи быть таким же идеальным правоприменителем: с одной стороны объективной, беспристрастной и точной Фемидой, с другой – проводником таких неопределённых понятий как мораль и справедливость. Иными словами, из «обработчика доказательств» судья превратился в «меру всех вещей».

Эта дихотомия необходимости сочетать объективное и субъективное проступает из статей 17, 305 и 307 УПК РФ, где принцип внутреннего (т. е. субъективного) убеждения

сосуществует с принципом объективности. Внутреннее убеждение при этом характеризуется как «вера в правильность знания»⁵, «голос, который говорит о правильности принятого решения»⁶. Свобода оценки доказательств, таким образом, по меткому определению Н. Г. Стойко, представляет собой «свободу усмотрения, ограниченную законом и совестью»⁷.

Объективность суда, таким образом, обеспечивается процессуальными рамками, а также уровнем профессионализма и правосознания самого судьи. Однако в определенных случаях указанные ограничители не срабатывают и судьи, под воздействием внутренних и внешних факторов (боязнь отмены приговора вышестоящим судом, угрозы и посягательства со стороны участников производства), **осознано** принимают решения, которые трудно назвать объективными⁸.

Помимо этого, существует ряд заблуждений, допускаемых судьями **неосознанно**. Их причиной являются когнитивные искажения – обусловленные нейрофизиологией мозга ошибки в мышлении и восприятии информации⁹. Одним из примеров подобных искажений

⁵ Лупинская П. А. Решения в уголовном судопроизводстве: теория, законодательство, практика. М.: Норма: Инфра-М, 2010. С. 173.

⁶ Вышинский А. Я. Теория судебных доказательств в советском праве. М.: Юрид. изд-во МЮ СССР, 1946. С. 113.

⁷ Уголовный процесс: учебник для бакалавриата юридических вузов / под ред. О. И. Андреевой, А. Д. Назарова, Н. Г. Стойко, А. Г. Тузова. Ростов н/Д.: Феникс, 2015. С. 47.

⁸ Подробнее об этих факторах: Горевой Е. Д. Внутреннее судейское убеждение в оценке доказательств по уголовным делам: моногр. М.: Юрлитинформ, 2008; Бурмагин С. В. Соответствие приговора внутреннему убеждению судьи // Сибирские уголовно-процессуальные чтения. 2017. №1. С. 13–20.

⁹ Боброва Л. А. Когнитивные искажения // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 3. Философия: Реферативный журнал. 2021. № 2. С. 70–72.

является так называемый Гало-эффект, заключающийся в распространении известных черт и характеристик человека на неизвестные¹⁰. Общее впечатление от обвиняемого в таком случае влияет на восприятие судьёй его частных особенностей, а некоторые известные и стигматизируемые склонности приводят к автоматически более негативной оценке поведения подсудимого, даже в случаях, когда они не связаны с событием преступления.

Возросшая интенсивность изучения когнитивных искажений (в т. ч. при анализе правовых и экономических отношений¹¹) вкупе с бумом развития технологий искусственного интеллекта (далее – ИИ) привели к появлению мнения о том, что внедрение ИИ в процесс принятия судебных решений позволит повысить объективность и точность последних. Обосновывается это тем, что ИИ не подвержен предрассудкам, а также может компенсировать и исправлять многие когнитивные ошибки судей. Так, например, если человек способен обрабатывать только ограниченное количество переменных,

то машина может принимать в расчёт практически неограниченный их объём¹².

Тем не менее, в настоящее время не существует технологий достаточно «умных» для того, чтобы служить полноценной заменой судьи¹³: современные системы ИИ могут определять лишь средние показатели на основе статистического регрессионного анализа (слабый ИИ) и не способны принимать комплексные и креативные решения (сильный ИИ)¹⁴. Более того, существует обоснованная точка зрения о принципиальной невозможности создать подобные технологии на основе применяемых в настоящее время принципов машинного обучения¹⁵.

Впрочем, концепция ИИ как интеллектуального помощника, а не замены судьи, уже находит своё применение во многих странах. Так, в 24 штатах США судами применяются алгоритмы для расчёта риска рецидивов (например, программа COMPAS). При разрешении конкретного дела алгоритм рекомендует судье применять такой размер наказания (или размер залога),

¹⁰ Lachman Sh., Bass A. R. A Direct Study of Halo Effect // The Journal of Psychology. 1985. Vol. 119, № 6. P. 535–540.

¹¹ Карапетов А. Г. Экономический анализ права: моногр. М.: Статут, 2016. С. 42.

¹² Why Smart Statistics Are the Key to Fighting Crime // TED. URL: <https://www.ted.com/talks/annemilgramwhysmartstatisticsarethekeytofightingcrime/transcript?language=en> (accessed: 01.05.22).

¹³ Сахнова Т. В. Цифровые технологии и правосудие: заметки на полях // Цифровые технологии и юрисдикционная деятельность: образ будущего правосудия по гражданским

делам / под ред. К. Л. Брановицкого, В. В. Яркова. Москва: Статут, 2022. С. 163–165.

¹⁴ Re R. M., Solow-Niederman A. Developing Artificially Intelligent Justice // Stanford Technology Law Review. 2019. Vol 22:2, № 242. P. 254.

¹⁵ Searle J. Is the Brain's Mind a Computer Program? // Scientific American. 1990. Vol. 262 (1). P. 26–31; Интервью с судьёй Участкового суда г. Эссен И. Бьяласс // LegalTech Cologne. Дата обновления: 21.02.22. URL: <https://anchor.fm/legaltech/episodes/53-KI-Systeme-in-der-Justiz---Wo-bestehen-Anwendungsfelder--Isabelle-Bialla-e1eirlp> (дата обращения: 01.05.22).

при котором у людей, обладающих сходными характеристиками с подсудимым, был зафиксирован минимальный риск совершения рецидива¹⁶. Сходные ИИ используются в судах Шанхая и Шаньдуня в Китае¹⁷. Базы данных судебных решений для возможного обучения ИИ уже разработаны в Японии¹⁸.

Объективность решений, предлагаемых ИИ-помощником, между тем, остаётся предметом сомнений и споров. Так, при независимом анализе всё той же программы COMPAS было установлено, что в качестве входных параметров она учитывала расу: осуждённым афроамериканского происхождения было рекомендовано назначить более длительные сроки наказания¹⁹. В Европе, в связи с этим, вопрос о внедрении ИИ в сферу принятия судебных решений рассматривается как потенциально рисковый и дискриминационный²⁰: ответственные за разработку законодательства в сфере ИИ комитеты Европарламента предлагают

ввести принципиальный запрет на использование подобных технологий при отправлении правосудия²¹.

Сторонники внедрения алгоритмов возражают против этого тем, что ИИ используется судом только лишь как инструмент, дающий рекомендации, а не предлагающий обязательные решения. Судья может и должен анализировать все обстоятельства дела, рассматривая рекомендации алгоритма лишь как одно из доказательств. Аналогичные выводы были озвучены Верховным судом штата Висконсин в деле о законности использования COMPAS. Суд указал, что алгоритм может быть использован при вынесении судебных решений в качестве вспомогательного и необязательного инструмента, а сам судья должен в обязательном порядке принимать во внимание другие материалы и доказательства по делу²².

С первого взгляда может показаться, что данные аргументы в пользу модели «тандема» судьи и алгоритма разумны: сильные стороны машины нивелируют слабые стороны

¹⁶ Christin A., Rosenblat A., Boyd D. Courts and predictive algorithms // Data & civil rights: a new era of policing and justice // Datasociety. URL: https://datasociety.net/wp-content/uploads/2015/10/Courts_and_Predictive_Algorithms.pdf (accessed: 01.05.22).

¹⁷ Пашенцев Д. А. Искусственный интеллект как субъект судебного толкования права // Образование и право. 2020. № 7. С. 200.

¹⁸ Nakagawa H. Die Strafzumessung in der Tatsacheninsatz / Grundfragen des Strafzumessungsrechts aus deutscher und japanischer Sicht. Freiburg: Mohr Siebeck, 2011. S. 209.

¹⁹ How We Analyzed the COMPAS Recidivism Algorithm / J. Larson, S. Mattu, L. Kirchner, Angwin J. // ProPUBLICA. URL: [https://www.propublica.org/article/how-we-](https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm)

[analyzed-the-compas-recidivism-algorithm](https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm) (accessed: 01.05.22).

²⁰ Završnik A. Big Data, Crime and Social Control. New York: Routledge. P. 131–153.

²¹ European Parliament committees support ban on predictive policing and criminal justice AI // Fairtrials. URL: <https://www.fairtrials.org/articles/news/european-parliament-committees-support-ban-on-predictive-policing-and-criminal-justice-ai/> (accessed: 01.05.22).

²² Решение по делу «штат Висконсин против v. Эрика Л. Лумиса // Официальный сайт Верховного суда штата Висконсин. Дата обновления: 17.04.17. URL: <https://www.wicourts.gov/sc/opinion/DisplayDocument.pdf?content=pdf&seqNo=171690> (дата обращения: 01.05.22).

судьи и наоборот. Так, алгоритм позволяет сократить влияние когнитивных искажений на судью. Последний же может обнаруживать дискриминационные или неправильные выводы машины и игнорировать их, оставляя за собой возможность принятия комплексных решений и неся ответственность за их правильность (*conditio humana*)²³.

Между тем, новейшие исследования показывают, что и такая модель не помогает решить проблемы минимизации когнитивных искажений и приводит к возникновению ещё одного – ошибки автоматизации (*automation bias*). Её первопричиной является обусловленная эволюцией склонность людей принимать решения, требующие меньших затрат сил и энергии. При появлении умного помощника, который предлагает готовое, но не обязательное решение определённого вопроса, человеку очень сложно уклониться от того, чтобы без дополнительной проверки или самостоятельной оценки ситуации принять решение, предлагаемое сложной алгоритмической системой²⁴. Другими словами, когда под рукой есть сложное техническое устройство, окружённое ореолом высоких технологий, человеком склонен сразу и полностью довериться тем рекомендациям, которые оно предлагает. Так, например, водители

автомобилей не перепроверяют маршрут, предложенный навигационной системой – намного удобнее безусловно следовать рекомендациям алгоритмов, а вместо самостоятельного выстраивания маршрута заняться более важными делами.

Исследования алгоритмических систем поддержки принятия решений в таких областях как медицина и пилотирование уже показали, что людям сложнее принимать решения, не соответствующие предлагаемым машиной. Там, где используются ИИ-помощники, люди склонны воздерживаться от самостоятельного сбора и оценки информации, а также игнорируют сведения, противоречащие результатам машинного анализа²⁵.

Такие инциденты уже начали проявляться в области принятия судебных решений. Так, в Дании в результате ошибки в работе программы, обрабатывавшей геолокационные данные мобильных устройств подозреваемых, в 2019 году был проведён пересмотр 10 000 уголовных дел, по итогам которого были отменены приговоры в отношении 32 осуждённых. При первоначальном рассмотрении указанных дел, суд в большинстве случаев чрезмерно доверял результатам работы программы даже

²³ Greco L. Richterliche Macht ohne richterliche Verantwortung: Warum es den Roboter- Richter nicht geben darf // Rechtswissenschaft. 2020. № 11. P. 21– 62.

²⁴ Automatisierte Risikoprognosen im Kontext von Bewährungsentscheidungen / F. Butz, S. Christoph, L. Sommerer, S. Harrendorf, J. Kaspar, K. Höffler // Bewährungshilfe –

Soziales, Strafrecht, Kriminalpolitik. 2021. Jg. 68, Heft 3, S. 254.

²⁵ Manzey D. Systemgestaltung und Automatisierung / P. Badke-Schaub, G. Hofinger, K. Lauche // Human Factors – Psychologie sicheren Handelns in Risikobranchen. Berlin. Heidelberg: Springer, 2012. S. 323.

тогда, когда в деле имелись доказательства, ставящие их правильность под сомнение²⁶.

Проведённые С. Алоном-Бакартом и М. Бусуйок эксперименты также показывают, что при осуществлении своей деятельности государственные служащие более склонны принимать на веру предлагаемые алгоритмами решения, если последние соответствуют общественным или их личным стереотипам²⁷.

Таким образом, *automation bias* переворачивает всё с ног на голову: из инструмента выработки рекомендаций ИИ превращается в систему, которой полностью отдана на «аутсорсинг» задача принятия решений²⁸. Помимо этого, ошибка автоматизации несёт в себе риск стимуляции, а не нивелирования осознанных стереотипов и когнитивных искажений судьи. Это, потенциально, может привести к тому, что:

1) дискриминационные настройки алгоритма будут воздействовать на судью, поддерживая и ещё больше убеждая его в правильности личных стереотипов;

2) судья будет без предварительной проверки использовать рекомендации алгоритма как «готовое решение», пытаясь

сэкономить время и силы в условиях загруженности судов и свойственного профессии психологического и физического напряжения;

3) неопределённые и оценочные понятия, такие как «справедливость», «обоснованность» и «достаточность доказательств» будут подводиться под предложенные алгоритмом результаты.

Все эти негативные черты модели «ИИ – судья» должны быть приняты во внимание не только при разработке алгоритмов, но и их интеграции в систему правосудия. Как человек, так и компьютер представляют собой системы обработки информации (*IPS, information processing system*), каждой из которых свойственны свои типы ошибок и особенностей²⁹. В настоящее время ученые концентрируются на проблемах интранспарентности и дискриминационного характера существующих алгоритмов. Однако не стоит забывать и о когнитивных искажениях, свойственных самому человеку, а также о таких ошибках мышления, как *automation bias*, которые могут появиться при интеграции алгоритмов в правосудие даже в, казалось бы, самой безопасной форме «рекомендательных инструментов». Так как существуют

²⁶ Ewald U. Volatilität digitaler Beweise - Herausforderung für die CyberStrafverteidigung // Rechtsanwälte für wirtschaftsstrafrecht in Kooperation. URL: <https://rechtsanwaelte-wirtschaftsstrafrechtberlin.de/volatilitaet-digitaler-beweiseherausforderung-fuer-die-cyberstrafverteidigung/> (accessed: 01.05.22).

²⁷ Alon-Barkat S., Busuioc M. Human-AI Interactions in Public Sector Decision-Making: «Automation Bias» and «Selective Adherence» to Algorithmic Advice // Journal of Public

Administration Research and Theory. DOI: <https://doi.org/10.7910/DVN/TQYJNF>.

²⁸ Manzey D. Systemgestaltung und Automatisierung / P. Badke-Schaub, G. Hofinger, K. Lauche // Human Factors – Psychologie sicheren Handelns in Risikobranchen. Berlin. Heidelberg: Springer, 2012. S. 323.

²⁹ Newell A., Simon H. A. Human Problem Solving. Chicago, 2019. P. 19.

сомнения в принципиальной возможности устранения ошибки автоматизации³⁰, перед учёными стоит задача выработать пути минимизации негативного влияния этого явления либо выступить против внедрения алгоритмов на сегодняшнем этапе развития технологий и права.

В противном случае, не найдя решений указанных проблем, уголовный процесс в XXI веке рискует вернуться к формальной теории доказательств: задачей суда будет

являться правильно загрузить данные в компьютер и интерпретировать полученный результат, а обвинение и защита будут заняты «подгонкой» доказательств под алгоритм. Пониманию права и искусству справедливости придёт на замену знание алгоритма и принципов оценки переменных. Излишне говорить о том, насколько такая ситуация будет противоречить принципам правового государства.

Список литературы

1. Алексеев С. С. Общая теория права. М.: Проспект, 2010. 565 с.
2. Боброва Л. А. Когнитивные искажения // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 3. Философия: Реферативный журнал. 2021. № 2. С. 69–79.
3. Бурмагин С. В. Соответствие приговора внутреннему убеждению судьи // Сибирские уголовно-процессуальные чтения. 2017. № 1. С. 13–20.
4. Вышинский А. Я. Теория судебных доказательств в советском праве. М.: Юрид. изд-во МЮ СССР, 1946. 248 с.
5. Горевой Е. Д. Внутреннее судейское убеждение в оценке доказательств по уголовным делам: моногр. М.: Юрлитинформ, 2008. 131 с.
6. Карапетов А. Г. Экономический анализ права: моногр. М.: Статут, 2016. 527 с.
7. Лупинская П. А. Решения в уголовном судопроизводстве: теория, законодательство, практика. М.: Норма: Инфра-М, 2010. 238 с.
8. Пашенцев Д. А. Искусственный интеллект как субъект судебного толкования права // Образование и право. 2020. № 7. С. 192–202.
9. Сахнова Т. В. Цифровые технологии и правосудие: заметки на полях // Цифровые технологии и юрисдикционная деятельность: образ будущего правосудия по гражданским делам / под ред. К. Л. Брановицкого, В. В. Яркова. Москва: Статут, 2022. С. 163–165.
10. Спасович В. Д. О теории судебно-уголовных доказательств. В связи с судоустройством и судопроизводством. М.: ЛексЭст, 2001. 93 с.
11. Уголовный процесс: учебник для бакалавриата юридических вузов / под ред. О. И. Андреевой, А. Д. Назарова, Н. Г. Стойко, А. Г. Тузова. Ростов н/Д.: Феникс, 2015. 445 с.

³⁰ Skitka L. J., Mosier K. L., Burdick M. D. Does Automation Bias Decision-Making? //

International Journal of Human-Computer Studies. 1999. Vol. 51. P. 1004.

12. Alon-Barkat S. Human-AI Interactions in Public Sector Decision-Making: «Automation Bias» and «Selective Adherence» to Algorithmic Advice / S. Alon-Barkat, M. Busuioc // *Journal of Public Administration Research and Theory*. DOI: <https://doi.org/10.7910/DVN/TQYJNF>.
13. Automatisierte Risikoprognosen im Kontext von Bewährungsentscheidungen / F. Butz, S. Christoph, L. Sommerer [et al.] // *Bewährungshilfe – Soziales, Strafrecht, Kriminalpolitik*. 2021. Jg. 68, Heft 3, S. 241– 259.
15. Christin A. Courts and predictive algorithms / A. Christin, A. Rosenblat, D. Boyd // *Data & civil rights: a new era of policing and justice* // *Datasociety*. URL: https://datasociety.net/wp-content/uploads/2015/10/Courts_and_Predictive_Algorithms.pdf.
16. Ewald U. Volatilität digitaler Beweise – Herausforderung für die CyberStrafverteidigung // *Rechtsanwälte für wirtschaftsstrafrecht in Kooperation*. URL: <https://rechtsanwaelte-wirtschaftsstrafrechtberlin.de/volatilitaet-digitaler-beweiseherausforderung-fuer-die-cyberstrafverteidigung/>.
17. Greco L. Richterliche Macht ohne richterliche Verantwortung: Warum es den Roboter- Richter nicht geben darf // *Rechtswissenschaft*. 2020. № 11. S. 21– 62.
18. Heghmanns M. Strafverfahren Strafrecht für alle Semester Grund- und Examenswissen kritisch vertieft. Springer, 2014. 791 s.
19. Lachman Sh. A Direct Study of Halo Effect / Sh. Lachman, A.R. Bass // *The Journal of Psychology*. 1985. Vol. 119, № 6. P. 535–540.
20. How We Analyzed the COMPAS Recidivism Algorithm / J. Larson, S. Mattu, L. Kirchner, J. Angwin // *ProPUBLICA*. URL: <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm>.
21. Manzey D. Systemgestaltung und Automatisierung / P. Badke-Schaub, G. Hofinger, K. Lauche // *Human Factors – Psychologie sicheren Handelns in Risikobereichen*. Berlin/Heidelberg: Springer, 2012. 365 s.
22. Nakagawa H. Die Strafzumessung in der Tatsacheninsatz / *Grundfragen des Strafzumessungsrechts aus deutscher und japanischer Sicht*. Freiburg: Mohr Siebeck, 2011. 259 p.
23. Newell A. Human Problem Solving / A. Newell, H. A. Simon. Chicago, 2019. 938 p.
24. Niehaus M. Das Verhör. Geschichte – Theorie – Fiktion. München: Wilhelm Fink Verlag, 2003. 592 s.
25. Re R. M. Developing Artificially Intelligent Justice / R. M. Re, Solow- A. Niederman // *Stanford Technology Law Review*. 2019. Vol 22:2, № 242. P. 242–289.
26. Searle J. Is the Brain's Mind a Computer Program? // *Scientific American*. 1990. Vol. 262 (1). P. 26–31.
27. Skitka L. J. Does Automation Bias Decision-Making? / L. J. Skitka, K. L. Mosier, M. D. Burdick // *International Journal of Human-Computer Studies*. 1999. Vol. 51. P. 991-1006.
28. Završnik A. Big Data, Crime and Social Control. New York: Routledge. 248 p.

Anatolii I. Zazulin

PhD (Law), Senior lawyer at INTELLECT Law Firm
(Yekaterinburg, Russian Federation)
a.zazulin@intellectmail.ru

AUTOMATION BIAS: ANOTHER PROBLEM OF INTEGRATION AI INTO JUSTICE

Abstract: This article is devoted to the topic of interaction between humans and artificial intelligence in the sphere of procedural decision-making, which has been little studied in the Russian legal literature. In a growing number of countries, attempts are being made to integrate the latest big data-technologies into the justice system: decision support software is being developed to calculate the amount of bail or criminal penalties. In order to explore the possible risks of the «AI – judge» model, author has analysed the history of criminal judicial decision-making and factors influence conscious or unconscious departures from the principle of objectivity. One such factor is automation bias - the human tendency to take the recommendations of AI algorithms «on faith». This article describes the possible negative legal consequences of ignoring the automation bias when integrating AI technology into justice.

Keywords: artificial intelligence, procedural decision, formal theory of evidence, cognitive bias, automation bias.

Карепанов Николай Васильевич
Кандидат юридических наук, доцент,
доцент кафедры криминалистики,
Уральский государственный юридический университет
имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
karepanovvv@gmail.com

ОСОБЕННОСТИ ТЕХНОЛОГИИ АГРЕГИРОВАНИЯ, ИССЛЕДОВАНИЯ И ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННО-ЦИФРОВЫХ СЛЕДОВ ПРЕСТУПЛЕНИЯ

Аннотация: В статье исследуются вопросы сущности, классификации электронно-цифровых следов, особенностей их обнаружения, исследования и использования. Прежде всего, в процессе обнаружения и исследования компьютерных следов извлекается не сама информация, а внешние признаки ее в виде сведений, которые в ней содержатся. Современные знания об электронных следах связаны с содержанием и структурой понятия «информация», анализ которых проводится в первой части статьи. Сведения, содержащиеся в электронных следах, могут быть зафиксированы на любом материальном носителе и проявляются в следующих понятиях: файл, сетевой адрес, доменное имя, электронное сообщение, электронный документ, информационная система, сайт в сети Интернет, страница сайта в сети Интернет, электронная подпись, программа для ЭВМ (компьютерная программа), база данных, электронный журнал, электронные денежные средства.

Носитель информации – это физическая среда, непосредственно хранящая информацию. Носитель информации – строго определенная часть конкретной информационной системы, служащая для промежуточного хранения или передачи информации.

Основа современных информационных технологий – это компьютер (ПК). Носители информации для него – это внешние запоминающие устройства (внешняя память). Их можно классифицировать по разным основаниям, в том числе по типу исполнения, материалу изготовления и т. п.

Технология поиска, обнаружения, фиксации и изъятия электронных доказательств в компьютерных устройствах основана на особенностях создания данных, их хранения и обмена с помощью электронных устройств.

Для определения технологии поиска необходимо знать услугами какого провайдера пользуется лицо, чья электронная почта подлежит обнаружению. Это можно сделать путем определения телефонного номера провайдера, с которым связывается абонент. Для доступа к серверу провайдера абонент может использовать и телефонные номера родственников, знакомых.

Другой путь может состоять в получении информации от провайдеров, работающих в регионе, где проживает интересующее поисковика лицо, о том, не имеется ли, но принадлежащих им серверах электронного почтового ящика конкретного субъекта.

Ключевые слова: электронно-цифровые следы, носитель информации, информационные технологии, технологии поиска, провайдер, электронная почта, сервер, электронный почтовый ящик, интегрированное компьютерное средство.

Для цитирования:

Карепанов Н. В. Особенности технологии агрегирования, исследования и использования электронно-цифровых следов преступления // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 86–104.

Информационные технологии появились уже в 1980-х г. и ознаменовали собой переход от аналоговых технологий к цифровым. Информационная эра (англ. Information Age, также известная как эра компьютеров или «информационная эпоха – электронная эпоха») – продолжающийся период в истории человечества с глобальным сдвигом от традиционной индустрии, установленной индустриальной революцией, к цифровой, компьютеризованной индустрии, основанной на трансфере информации¹. Благодаря этому как для законопослушных граждан, так и для преступников возникают широкие возможности по свободному обмену любой информацией с мгновенным доступом к различного рода знаниям.

В современном мире неотъемлемой частью деятельности человека становится работа с цифровыми устройствами: персональными компьютерами,

ноутбуками, планшетами, мобильными телефонами, смартфонами и многими другими. Сегодня практически все электронно-цифровые устройства объединяются в глобальную сеть Интернет. Причём каналы связи с сетью разнообразны: проводные (оптоволоконные), беспроводные сети (мобильные, спутниковые каналы связи).

Технический прогресс неминуемо проникает в криминальную среду, отражается на преступной деятельности. Мы сегодня наблюдаем стремительный рост преступлений, совершаемых с использованием цифровых технологий. Совершенно естественно, что в практике расследования таких преступлений возникает потребность в теоретическом осмыслении сущности и понятии компьютерных следов, выработке поисковых методов их обнаружения, агрегирования, исследования и использования.

¹ Информационная эра // Википедия – свободная энциклопедия. URL:

https://ru.wikipedia.org/wiki/Информационная_эра (дата обращения: 01.05.2022).

Компьютерные следы выражаются в электронной (цифровой) форме. Строго говоря, как мы в дальнейшем будем утверждать, такая информация неразрывно связана с её носителем и скрыта. В процессе обнаружения и исследования компьютерных следов извлекается не сама информация, а её внешние признаки в виде сведений, которые в ней содержатся. Именно они (признаки) и являются следами — проявлением информации в материальном мире.

Поскольку термин «информация» является сущностью компьютерных следов и в настоящее время неразрывно связан с компьютерными и иными, в том числе, цифровыми технологиями, мы будем оперировать в исследовании знаний о следах этой категории словом «информация».

Современные знания об электронных следах связаны с содержанием и структурой понятия «информация». Последняя состоит из трёх элементов: источника информации, потребителя и среды передачи. Носителем информации является сообщение, то есть кодированный эквивалент события, зафиксированный источником информации и выраженный с помощью последовательности условных физических символов, которые образуют определённую упорядоченную совокупность. Физическими силами могут выступать алфавиты. Передача информации осуществляется посредством каналов связи в форме сигнала, приемлемого для конкретного канала связи. Под сигналом понимают знак,

определённый физический процесс или явление, которые распространяются в определённом канале связи и несут в своём содержании сообщение о том или ином событии.

Сигнал имеет определённую смысловую нагрузку, отличающуюся от самого факта поступления информации. Физическая регистрация сигнала не означает, что информация дошла к потребителю. Информация тогда получена потребителем, когда он сам извлёк из неё понятный ему смысл. Сигнал не всегда имеет прямую физическую связь с отражаемым событием, о котором он несёт информацию потребителю, информация здесь выступает как свойство объектов (явлений) порождать многообразие состояний. Эти состояния через отражения передаются от одного объекта к другому и таким образом запечатлеваются в его структуре.

Информация в отличие от других процессов действительности не носит энергетического характера (количество и качество переданной информации не зависят от количества затраченной на её передачу энергии), может направляться и контролироваться при помощи небольших количеств энергии. Между тем, следует согласиться с А. Н. Колмогоровым, который обозначал информацию как абстрактную

величину, не существующую в физической реальности².

Понятие «информация» гносеологически тесно связано с понятием «компьютерная информация». Последняя является одной из объективных форм существования информации электронно-цифровой формы. Основопологающим определением компьютерной информации считается описание её через информацию, циркулирующую в вычислительной среде, зафиксированной на физическом носителе в форме, доступной восприятию электронно-вычислительной машиной, или передающейся по телекоммуникационным каналам связи³.

Современное понимание этого термина сформулировал В. Б. Вехов, который определил компьютерную информацию в качестве «сведений (сообщений, данных), находящихся в электронно-цифровой форме, зафиксированных на материальном носителе с помощью электромагнитных взаимодействий, либо переданных по каналам связи посредством электромагнитных сигналов»⁴.

Криминалистический алгоритм информационных процессов выглядит следующим образом⁵.

1. Отображение как носитель образовавшихся в нем данных о свойствах и признаках отображаемого объекта в акте познания может выполнять функцию источника сведения о нём, а также о механизме самого взаимодействия.

2. Под собственно информацией следует понимать данные, которые могут быть выделены познающим субъектом в том или ином отображении познаваемого объекта.

3. Несмотря на то, что само по себе понятие «информация» относится к числу абстрактных, проявляется информация всегда в материально-энергетической форме, в частности в виде сигналов, которые могут иметь различную физическую форму (сигнал в информационном пространстве выполняет функцию переносчика информации от её источника к приёмнику и далее, к субъекту – потребителю информации).

4. Передача информации является одной из фаз информационного процесса, присущего информационной системе.

5. Собственно информационный процесс начинается с восприятия и фиксации информации, содержащейся в том или ином источнике. Завершается он формированием сигнала, с помощью структуры которого и передаётся

² Блюменау Д. И. Информация и информационный сервис. Л.: Система, 1989. С. 14.

³ Карась И. З. Экономический и правовой режим информационных ресурсов // Право и информатика / под ред. Е. А. Суханова. М.: Изд-во МГУ, 1990. С. 40.

⁴ Вехов В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки. Волгоград: ВА МВД России, 2008. С. 71.

⁵ Правовая информатика и кибернетика: учебник / под ред. Н. С. Полевого. М.: Юридическая литература, 1993. С. 27–31.

информация, которая выражается в дискретной форме.

6. На принципе передачи информации с помощью таких сигналов, преобразованных языком программирования в цифровую систему, и функционирует, например, электронно-вычислительная техника.

7. Информационный процесс в любой системе начинается с восприятия и выделения нужной информации, а сама информация представляет собой содержание сигнала, который был удобен для её передачи в соответствии с каналом связи различной физической природы.

8. Передача информации как фаза информационного процесса есть не что иное, как перенос информации на расстояние, её движение во времени и пространстве посредством того или иного сигнала.

Физическая природа каналов связи может быть механической, электрической, воздушной и т. п. Приём информации осуществляется с помощью органов чувств и является вторичным, как и приём техническими устройствами. Обработка же информации протекает по-разному. Например, человек, осуществляя смысловую и логическую обработку, не обосновывает этот процесс жёсткой системой формализованных правил.

Сведения, содержащиеся в электронных следах, могут быть зафиксированы на любом материальном носителе. Это может сделать человек или (и) автомат (без участия человека по установленному алгоритму). В обоих случаях сведения

могут быть представлены в электронном виде в форме компьютерной информации независимо от средств хранения, обработки и передачи.

Общими признаками таких следов являются:

1) представлены в закодированном виде в электронной форме;

2) опосредованы через технический материальный носитель, вне которого не существуют;

3) доступ к ним могут иметь одновременно несколько субъектов;

4) их возможно просто и быстро преобразовать в неэлектронные формы и обратно;

5) копируются на различные виды электронных носителей, передаются на любые расстояния;

6) собираются, исследуются и используются только с помощью специальных научно-технических средств хранения, обработки и передачи компьютерной информации, информационно-телекоммуникационных сетей и оконечного оборудования.

Информационная сущность фиксации следов, находящихся в электронно-цифровой форме, заключается в следующем⁶.

1. Производится перекодировка следовой компьютерной информации, содержащейся на оригинальном материальном носителе, в форму, доступную для восприятия её человеком (выводится текстом на монитор компьютерного устройства или прослушивается как фонограмма).

⁶ Электронные носители информации в криминалистике: монография / И. В. Александров, Д. В. Бахтеев, В. Б. Вехов [и

др.]. Москва: Издательство «Юрлитинформ», 2017. С. 135–138.

2. Компьютерная информация изымается вместе с её материальным носителем либо копируется на отличный от оригинала материальный носитель.

3. Обеспечивается сохранение, накопление и неоднократное использование компьютерных следов (например, по реквизитам файла электронного сообщения можно установить дату, время, электронный адрес, идентификатор компьютерного передающего компьютерного устройства, абонентский номер этого устройства в компьютерной сети оператора связи, физический адрес нахождения компьютерного устройства, возможные следы подготовки указанного сообщения на данном техническом устройстве).

4. Обеспечивается возможность отбора информации о событии: фиксируется не вся компьютерная информация, а лишь необходимая.

5. Запечатлевается не только сама следовая компьютерная информация, но и информация о путях, способах её получения.

Электронные следы проявляются в следующих понятиях: *файл, сетевой адрес, доменное имя, электронное сообщение, электронный документ, информационная система, сайт в сети Интернет, страница сайта в сети Интернет, электронная подпись, программа для ЭВМ (компьютерная программа), база данных, электронный журнал, электронные денежные средства.*

Следы (сознание людей, материальные объекты) содержат определённую информацию, которая извлекается в виде сведений, для познания событий прошлого. Источниками сведений электронной переписки (следами) являются:

- письма, пересылаемые по электронной почте (e-mail);
- личные сообщения в социальных сетях («ВКонтакте», «Одноклассники» и т. п.);
- переписка с использованием специального ПО (мессенджеров), таких как Skype, Viber, WhatsApp, Jabber, ICQ и т. п.;
- текстовые сообщения, передаваемые с помощью сотовой связи (СМС, ММС)⁷.

Приведённый перечень не является исчерпывающим. Научно-технический прогресс способствует появлению новых способов передачи электронных сообщений.

Образование следов электронной переписки определяется механизмом работы электронной почты. Так, отправленное с бесплатного почтового сервера электронное сообщение проходит следующие этапы:

- 1) почтовый сервер-отправитель;
- 2) сеть Интернет;
- 3) почтовый сервер-получатель.

Местами образования (нахождения) электронной почты могут быть:

- компьютер (смартфон) лица, отправляющего электронную почту;

⁷ Электронные носители информации в криминалистике: монография / И. В. Александров, Д. В. Бахтеев, В. Б. Вехов [и

др.]. Москва: Издательство «Юрлитинформ», 2017. С. 145–146.

- сервер, с которого отправлено письмо;
- сервер, получающий сообщения электронной почты (у оператора связи, Интернет-провайдера на почтовом сервере отправителя или получателя);
- компьютер (иное электронное устройство) лица, которому адресована электронная корреспонденция.

Сеть ЭВМ (computer network) – это совокупность связного и коммуникационного оборудования, протоколов и программных средств, объединяющих несколько ЭВМ и терминалов в единую вычислительную систему⁸. Обмен сведениями между ЭВМ и другими компьютерными устройствами обеспечивается *сетью электросвязи* (технологической системой, включающей в себя средства и линии связи и предназначенной для электросвязи или почтовой связи). При этом *средства связи* – это технические и программные средства, используемые для формирования, приёма, обработки, хранения, передачи, доставки сообщений электросвязи или обеспечения функционирования сетей связи,

включая технические системы и устройства с измерительными функциями (т. е. локальные компьютерные сети объединяются в глобальные посредством сетей электросвязи).

Сети электросвязи базируются на ЭВМ и программных средствах, поскольку это любые излучения, передача или приём сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической или другим электромагнитным системам. Поэтому сеть электросвязи также является информационно-телекоммуникационной сетью.

Как источник получения следов её можно классифицировать по критерию установления возможных мест локализации электронно-цифровых следов и географического нахождения мест событий (*локальная, местная*⁹, *территориальная*¹⁰, *региональная или территориально распределённая*¹¹, *национальная, глобальная*).

Электронно-цифровые следы образованные и сохранённые конкретным видом компьютерной сети

⁸ Борковский А. Б. Англо-русский словарь по программированию и информатике (с толкованиями): около 6000 терминов. М.: Московская международная школа переводчиков, 1992. С. 61.

⁹ Правила оказания услуг местной, внутризоновой, междугородной и международной телефонной связи (п. 2 ч. 1): утв. постановлением Правительства РФ от 18 мая 2005 г. № 310 // ИПС «Гарант». URL: <https://base.garant.ru/58163854/> (дата обращения: 01.05.2022).

¹⁰ Правила оказания услуг местной, внутризоновой, междугородной и

международной телефонной связи (п. 2 ч. 1): утв. постановлением Правительства РФ от 18 мая 2005 г. № 310 // ИПС «Гарант». URL: <https://base.garant.ru/58163854/> (дата обращения: 01.05.2022).

¹¹ Правила оказания услуг местной, внутризоновой, междугородной и международной телефонной связи (п. 2 ч. 1): утв. постановлением Правительства РФ от 18 мая 2005 г. № 310 // ИПС «Гарант». URL: <https://base.garant.ru/58163854/> (дата обращения: 01.05.2022).

указывают на оператора связи (провайдера услуг Интернет), сведения о месте нахождения оконечного компьютерного устройства (рабочей станции сети) и лично абонента (пользователя услугами связи, с которым заключён договор об оказании таких услуг при выделении для этих целей абонентского номера или уникального кода идентификации¹²).

Важным, как полагает В. Б. Вехов, является выделение в электронных следах такого термина, как «дорожка электронно-цифровых следов» (по аналогии с дорожкой следов ног и обуви человека, запаховой дорожкой, остающейся на пути следования объекта)¹³.

Под дорожкой электронно-цифровых следов следует понимать систему образования следов в информационно-телекоммуникационной сети, состоящую из нескольких последовательно расположенных во времени и логически взаимосвязанных записей о прохождении компьютерной информации по линиям связи через коммутационное оборудование оператора(ов) связи от компьютера

передатчика до компьютера приёмника¹⁴.

Элементами дорожки электронно-цифровых следов можно считать следующие девять видов записей:

1. записи в файловой системе (реестре операционной системы и др.) компьютера передатчика, свидетельствующие о подключении и использовании модема¹⁵, либо записи, содержащиеся в модуле идентификации абонента связи оператора (IMPI, Ki, IMSI- код, MIN, TSN и другие идентификаторы);

2. записи в памяти компьютера или аппарата связи (например, в электронной записной книжке аппарата сотовой радиотелефонной связи), содержащие сведения об отправленной в адрес приёмника компьютерной информации или сеансе работы в компьютерной сети (*Соединение по компьютерной сети (сеанс связи)*) – это установленное в результате вызова или предварительно установленное взаимодействие между средствами связи, позволяющее абоненту и (или) пользователю передать и (или) принимать голосовую и (или) неголосовую информацию¹⁶;

¹² Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» (п. 1 ст. 2) // ИПС «Гарант». URL: <https://base.garant.ru/186117/> (дата обращения: 01.05.2022).

¹³ Электронные носители информации в криминалистике: монография/ И. В. Александров, Д. В. Бахтеев, В. Б. Вехов [и др.]. Москва: Издательство «Юрлитинформ», 2017. С. 184.

¹⁴ Правила применения средств связи для передачи голосовой и видеоинформации по сетям передачи данных (подпункт 4 пункта 3): утв. Приказом Министерства

информационных технологий и связи РФ от 10 января 2007 г. № 1 // ИПС «Гарант». URL: <https://base.garant.ru/190515/> (дата обращения: 01.05.2022).

¹⁵ Практические основы компьютерно-технической экспертизы/ А. Б. Нехорошева и др. Саратов: Научная книга. 2007 (раздел 2).

¹⁶ Правила оказания услуг связи по передаче данных: утв. постановлением Правительства РФ от 23 января 2006 года № 32 (п.2) // ИПС «Гарант». URL: <https://base.garant.ru/77323269/> (дата обращения: 01.05.2022).

3. записи в памяти компьютерного устройства контроля, авторизации и аутентификации абонентов в сети оператора(ов) связи (контроллера сигналов, гейткипера для протокола H.323, сервера регистрации соединений абонентов и сервера определения месторасположения абонентов для протокола SIP-прокси-сервера)¹⁷;

4. записи в системе учёта данных для начисления платы за оказанные услуги связи, автоматически регистрирующей основные данные, имеющие криминалистическое значение¹⁸:

- категорию и номер вызывающего абонента или адресную информацию вызывающей стороны,
- номер вызываемого абонента (службы) или адресную информацию вызываемой стороны,
- дату (день, месяц, год) и время начала соединения – сеанса связи (час, минута, секунда),
- продолжительность соединения или время окончания

соединения – сеанса связи (час, минута, секунда);

5. используемые в соединении услуги, объём передаваемой компьютерной информации в случае установления соединений для передачи данных;

6. записи, автоматически регистрируемые в журнале событий компьютерной сети, который находится на сервере оператора связи в ведении администратора сети¹⁹;

7. записи, автоматически образующиеся в памяти транзитных устройств различных операторов при сопряжении с их сетями передачи данных по протоколу IP (от англ. *Internet Protocol*), выполняющие функции маршрутизации, управления сигнализацией, контроля, авторизации абонентского терминала, которым воспользовался абонент, и управления пакетами IP (по протоколам H.323/SIP/H.248/MEGACO), содержащими голосовую, видео и мультимедиаинформацию. В них содержится сетевое имя компьютера

¹⁷ Правила оказания услуг связи по передаче данных: утв. постановлением Правительства РФ от 23 января 2006 года № 32 (п. 2, 3) // ИПС «Гарант». URL: <https://base.garant.ru/77323269/> (дата обращения: 01.05.2022); Правила применения средств связи, используемых для обеспечения доступа к информации информационно-телекоммуникационных сетей, передачи сообщений электронной почтой и факсимильных сообщений: утв. Приказом Министерства информационных технологий и связи РФ от 11 декабря 2006 года № 166 (п. 3) // ИПС «Гарант». URL: <https://base.garant.ru/190379/> (дата обращения: 01.05.2022).

¹⁸ Правила применения оборудования коммуникации систем подвижной радиотелефонной связи Ч. II. Правила

применения оконечно-транзитных узлов связи сетей подвижной радиотелефонной связи стандарта GSM 900/1800 (Приложение 8, пп. 4–8): утв. Приказом Министерства информационных технологий и связи РФ от 31 мая 2007 года № 58 // ИПС «Гарант». URL: <https://base.garant.ru/191404/> (дата обращения: 01.05.2022).

¹⁹ Правила применения средств связи, используемых для обеспечения доступа к информации информационно-телекоммуникационных сетей, передачи сообщений электронной почтой и факсимильных сообщений (п. 20.6): утв. Приказом Министерства информационных технологий и связи РФ от 11 декабря 2006 № 166 // ИПС «Гарант». URL: <https://base.garant.ru/190379/> (дата обращения: 01.05.2022).

передатчика – так называемый IP-адрес, адрес электронной почты и другая криминалистически значимая информация²⁰;

8. записи в памяти серверов (FTP, SMTP, POP3 и др.) оператора связи, обслуживающего абонентский терминал приёмника, о входящих на него вызовах, соединениях и передачах компьютерной информации (электронных сообщений, электронных почтовых отправок и др.), а также дистанционном управлении его информационными ресурсами;

9. записи в файловой системе (реестре операционной системы и др.) компьютера приёмника о параметрах изменения подключения модема, настроек браузера, а также о нарушениях режима работы или деактивации средств защиты портов и компьютерной информации;

10. записи в памяти компьютера или аппарата связи приёмника (например, в электронной записной книжке аппарата сотовой радиотелефонной связи), содержащие сведения о получении компьютерной информации, вредоносных программах, несанкционированном изменении системного и прикладного программного обеспечения, а также компьютерной информации приёмника либо сбоях в работе ЭВМ,

его программного обеспечения и периферийного оборудования.

Идея, высказанная В. Б. Веховым, назвать совокупность представленных записей «дорожкой электронно-цифровых следов», достаточно интересная. Вместе с тем, когда мы говорим о дорожке следов обуви или ног или запаховых проявлений, речь идёт об одном и том же объекте, повторяющемся несколько раз. В случае с компьютерными записями, повторений не наблюдается, все указанные записи различны по своему содержанию, времени и пространству. В этом случае может быть более приемлемо назвать последовательное наступление таких событий «цепочкой следов», где звенья одной цепочки связаны между собой, но могут различаться до некоторой степени.

Носитель информации – это физическая среда, непосредственно хранящая информацию; это строго определённая часть конкретной информационной системы, служащая для промежуточного хранения или передачи информации²¹.

Основа современных информационных технологий – это компьютер (ПК). Носители информации для него – внешние запоминающие устройства (внешняя память). Их можно классифицировать по разным основаниям, в том числе по

²⁰ Правила применения средств связи для передачи голосовой и видеoinформации по сетям передачи данных (п. 4): утв. Приказом Министерства информационных технологий и связи РФ от 10 января 2007 года № 1 // ИПС «Гарант». URL: <https://base.garant.ru/190515/> (дата обращения: 01.05.2022).

²¹ Кучин О. С. Виды носителей информации, изучаемой наукой криминалистикой // Электронные носители информации в криминалистике: монография/ под ред. докт. юрид. наук О. С. Кучина. М.: Юрлитинформ, 2017. С. 187.

типу исполнения, материалу изготовления и т. п.

Наиболее известны:

1. Ленточные носители информации (тонкая гибкая магнитная лента, носитель магнитной записи, состоит из основы и магнитного рабочего слоя). Рабочие свойства характеризуются её чувствительностью при записи и искажениями сигнала в процессе записи и воспроизведения. Наиболее широко применяется многослойная магнитная лента с рабочим слоем из игольчатых частиц магнитно-твёрдых порошков гамма-окиси железа (γ -Fe₂O₃), двуокиси хрома (CrO₂) и гамма-окиси железа, модифицированной кобальтом, ориентированных обычно в направлении намагничивания при записи;

2. Дисковые носители информации, которые относятся к машинным носителям с прямым доступом. Понятие «прямой доступ» означает, что компьютер может «обратиться» к дорожке, на которой начинается участок с искомой информацией или куда нужно записать новую информацию (гибкие магнитные диски или флоппи-диски или дискеты – НГМД; жесткие магнитные диски или винчестеры или «винты» – НЖМД; оптические компакт-диски: CD-ROM (*Compact Disk ROM*), DVD-ROM; магнитоскопические диски и др.);

3. FLASH- технологии или flash-диски, флешки, где информация хранится не на дисках, а в микросхемах памяти. Флэш-память (англ. *Flash-Memory*) – это разновидность твердотельной полупроводниковой

энергонезависимой перезаписываемой памяти.

Хранение информации – это способ распространения информации в пространстве и времени. Для компактного хранения информации и быстрого доступа к ней предназначен компьютер, где информация содержится в виде данных с помощью различных устройств: регистров, процессоров, регистровой КЭШ-памяти и др. Можно выделить оперативную память (ОЗУ) и постоянную память. Оперативной памятью называется запись данных в электронные микросхемы. Она состоит из ячеек, в каждой из которых может храниться один байт данных. У каждой ячейки есть свой адрес (адресные ячейки), компьютер, отправляя данные, запоминает адреса их размещения, по которым потом их находит.

Поскольку один байт состоит из восьми битов, то в каждой адресной ячейке восемь битовых ячеек, каждая из которых хранит электрический заряд. Заряды хранятся несколько долей секунды, (они быстро «стекают») и данные утрачиваются.

Для постоянного хранения данных используют носители информации. Большая часть информации, к которой необходим постоянный доступ, хранится на жёстком диске. Чтобы записать и потом прочесть данные им должен быть присвоен адрес.

Вся информация хранится в виде файлов. Для управления доступом к информации существует файловая система (их имеется несколько типов). Структура данных на диске зависит от типа файловой системы, которые

включают загрузочную запись операционной системы, каталоги и файлы, и исполняют три главные функции:

- 1) отслеживание занятого и свободного места;
- 2) поддержка имён каталогов и файлов;
- 3) отслеживание физического местоположения каждого файла на диске.

Различные файловые системы используются различными операционными системами (ОС). Некоторые ОС могут распознавать только одну файловую систему, другие – несколько. Наиболее распространены следующие файловые системы: FAT (*File Allocation Table*); FAT32 (*File Allocation Table32*); NTFS (*New Technology File System*); HPFS (*High Performance File System*); NetWare File System; Linux Ext2 и Linux Swap.

Все носители информации являются потенциальными следовыми носителями. Задачей является установление связи носителя и находящейся в нём информации с непосредственным автором или пользователем.

Технология поиска, обнаружения, фиксации и изъятия электронных доказательств в компьютерных устройствах основана на особенностях создания данных, их хранения и обмена с помощью электронных устройств²².

Так, электронные сообщения могут передаваться на значительные расстояния в течение нескольких минут. Архитектура сетевых протоколов TCP/IP, на базе которых построена сеть Интернет, предназначена специально для объединённой сети. Сеть может состоять из разнообразных подсетей, соединённых друг с другом шлюзами. В качестве подсетей могут выступать самые различные локальные (Token Ring, Ethernet, пакетные радиосети и т. п.), национальные, региональные и специализированные, а также другие глобальные сети. К этим сетям могут подключаться компьютеры разных типов. Каждая подсеть может принять пакет информации и доставить его по указанному адресу в этой конкретной подсети²³.

Сущность Интернета состоит в том, что все компьютеры, включённые во всемирную сеть, работают в автоматическом режиме, без участия людей. Промежуточные компьютеры, пересылающие электронную почту, не имеют информации о месте нахождения отправителя и получателя. Их задача, переслать пакет другому компьютеру, который находится к получателю ближе, чем они сами.

Процесс создания компьютерных сообщений для пересылки по электронной почте (e-mail) начинается с запуска программы и работы пользователя на клавиатуре.

²² См. Способы получения доказательств и информации в связи с обнаружением (возможностью обнаружения) электронных носителей: учебное пособие / В. Ф. Васюков, Б. Я. Гаврилов, А. А. Кузнецов [и др.]; под общ. ред. Б. Я. Гаврилова. М.: Проспект, 2017.

²³ Швоев М. И. Технология работы в компьютерных сетях // Информационные технологии в юридической деятельности. М.: Юрайт, 2013. С. 347.

В результате в окне программы формируется письмо, а после его готовности даётся команда «отправить».

Программа отправки электронной почты подключается к сети Интернет, сервер-отправитель связывается с сервером-получателем и передаёт текст сообщения (если используется сервер провайдера или бесплатный почтовый интернет-сервер (на таких серверах существуют свои (встроенные) программы работы с электронной почтой) то пользователь заходит на этот сервер и там набирает) текст письма. Лицо, которому предназначено компьютерное сообщение (письмо), загружает программу работы с электронной почтой для входа в сеть Интернет. Программа переписывает почту с сервера получателя (если это сервер провайдера или бесплатный почтовый интернет-сервер, то не обязательно загружать программу для работы с электронной почтой потому, что там есть своя).

Исходя из приведённой технологической схемы, сообщения электронной почты могут быть на:

- 1) компьютере отправителя;
- 2) сервере отправителя;
- 3) сервере получателя;
- 4) компьютере получателя.

Поиск содержания электронной почты может осуществляться через её бесплатный сервер на компьютере или с помощью программ работы с электронной почтой, местами его хранения²⁴ могут быть:

а) папка «входящие» (в ней хранится вся поступающая корреспонденция до момента её удаления (может быть восстановлена);

б) папка «исходящие» (в ней хранится информация, подготовленная к отправлению, а при отправлении – она удаляется);

в) папка «отправленные» (в ней хранятся копии переданных с данного компьютера сообщений до их удаления пользователем или автоматически). Пользователем могут создаваться и другие папки практически под любыми именами²⁵.

Приведённая технология сосредоточения информации электронной почты относится к компьютеру, получающему электронному почту.

Структура адреса электронной почты зависит от вида, определяемого сетью, в которую отправляется письмо (Интернет-сеть, Интернет – внутренние сети предприятий, учреждений и т. д.). Самые распространённые адреса электронной почты сети Интернет состоят из двух частей, разделённых символом @ («собака»). Первая часть – идентификатор пользователя, написанный латинскими буквами (он может быть любым). Что касается почтовых ящиков, предоставляемых по заключённому договору на сервере провайдера, то они (имена) могут даваться провайдером. Как правило, это имя пользователя для входа в интернет. Второй элемент – доменный адрес почтового сервера нахождения

²⁴ Microsoft Outlook Express, Netscape Messenger, The Bat – как правило, названия папок хранения электронной почты этих программ совпадают.

²⁵ Жардев П. А., Шаров Ю. В. Методы и способы получения доказательственной информации с электронных носителей. Хабаровск, 2013. С. 52–57.

электронного почтового ящика (например, mail.ru), то есть места, где находится почтовый ящик. Местами нахождения могут быть:

1) почтовые ящики, выделяемые по договору с провайдером на его сервере, как правило, такой сервер находится по месту нахождения провайдера;

2) почтовые ящики, находящиеся на бесплатном почтовом сервере и имеющие своего владельца, реквизиты которого, как правило, указаны на главной веб-странице внизу. Главная (или стартовая) страница сервера – это та, которая открывается первой после входа на сервер (то есть непосредственно после введения адреса, например: www.mail.ru).

Интернет, кроме обмена информацией между абонентами сети и использования баз данных сети предоставляет множество других услуг²⁶.

Для определения технологии поиска необходимо знать услугами какого провайдера пользуется лицо, чья электронная почта подлежит обнаружению. Это можно сделать путём определения телефонного номера провайдера, с которым связывается абонент. Для доступа к серверу провайдера абонент может использовать и телефонные номера родственников, знакомых.

Другой путь может состоять в получении информации от провайдеров, работающих в регионе, где проживает интересующее поисковика лицо, о том, не имеется ли, на принадлежащих им серверах электронного почтового ящика конкретного субъекта.

Информация об адресе электронной почты содержится в папках официальных бланков юридического лица, визитных карточках, еженедельниках, записных книжках. Сообщения, передаваемые от одного лица другому, могут быть в форме переписки, телефонных переговоров, почтовых и телеграфных сообщений, факсимильных, компьютерных, пейджинговых, радиовещательных сообщений (информации, хранимой, обрабатываемой и передаваемой по сетям электронной связи в виде последовательностей аналоговых или цифровых сигналов).

Под электросвязью понимаются «любые излучения, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам»²⁷.

При использовании интегрированного компьютерного средства мобильный телефон является

²⁶ Шурухнов Н. Г. Технология и процессуальный порядок выемки электронной почты (Е-mail) при расследовании отдельных видов преступлений // Нюрнбергский процесс – приговор фашизму: материалы Международной науч.-практ. конференции в рамках праздничных мероприятий,

посвященных 70-летию Победы в Великой Отечественной войне, 2015. С. 339–346.

²⁷ Федеральный закон «О связи» от 7 июля 2003 г. № 126-ФЗ (с изм. и доп., вступ. в силу с 10.01.2016) // ИПС «Гарант». URL: <https://base.garant.ru/186117/> (дата обращения: 01.05.2022).

неотъемлемым компонентом, в связи с чем возникает необходимость его поиска. В целях обнаружения компьютерных устройств и электронных носителей информации следует прибегнуть к помощи операторов средств сотовых систем подвижной связи (СССПС), которые определяют базовую станцию, а соответственно, примерное местоположение включённого мобильного телефона.

В зависимости от места сосредоточения информацию средств сотовых систем подвижной связи В. А. Козинкин подразделяет на содержащуюся:

а) в пользовательском оборудовании (абонентской станции, абонентском устройстве) в различных файлах: текстовых (63 %), фото и видео (28 %), звуковых (9 %);

б) в оперативно-информационных системах и центрах коммуникации оператора подвижной связи²⁸.

Следы, содержащие сведения об обстоятельствах события, обстановке использования мобильного телефона, о лицах, использовавших мобильные телефоны, интенсивности их использования, можно обнаружить на:

- мобильных станциях (сотовых телефонах);
- SIM-картах;
- протоколах детализации соединений;
- флэш-картах и других комплектующих мобильных телефонов;

- картах экспресс-оплаты;
- паспортах, упаковочной таре, гарантийном талоне (атрибуты приобретения мобильного телефона в конкретной точке), по которым можно получить сведения об IMAI – коде, особенностях этого устройства.

В процессе осмотра средств связи могут быть обнаружены электронные следы, в том числе свидетельствующие о его использовании:

- специальные программы;
- заданные установки, настройки на определённый режим;
- данные, содержащиеся в памяти компьютерного устройства (записи, отчеты и др.);
- информация о подключении периферийного оборудования и т. п.

При этом следует прежде всего ориентироваться на установление: абонентских и идентификационных номеров, под которыми работает телефон в сети связи, другой технической информации, участвующей в процессе идентификации телефона в сети; программного обеспечения, с помощью которого осуществляются сканирование, декодирование, запись и хранение необходимых данных, продуктов применения указанных специальных программ и т. п.; данных, относящихся к установкам телефона, тонам, заставкам и т. п., которые

²⁸ Козинкин В. А. Использование в расследовании преступлений информации, обнаруживаемой в средствах сотовых систем

подвижной связи: автореф. дис. ... канд. юрид. наук. М., 2009. С. 15–16.

удостоверяют отдельные обстоятельства²⁹.

Исследование информационно-коммутационного содержания сотового аппарата проводится, ориентируясь на его «Меню», что позволяет получить различные электронные следы³⁰.

Электронные следы могут быть обнаружены при исследовании SIM-карты. Для выяснения внутренней спецификации (объём имеющейся информации, структура и название данных, дата и время их создания и т. п.) необходимо выяснение защитного индивидуального идентификационного номера (PIN-кода). SIM – карта является носителем следов и при удалении с неё данных, поскольку информация не уничтожается полностью. При этом блоку данных присваивается показатель возможности производства записи другой информации поверх него. Фактически, когда удаляются текстовые сообщения или список звонков, они сохраняются на самой карте и ещё долго доступны для получения³¹.

Специфика расследования исследуемых преступлений указывает на то, что основная часть выявляемых

цифровых следов формируется на этапе приёма сообщения о преступлении. Сегодня достаточно чётко выработаны многочисленные рекомендации по проведению доследственных проверок и отдельных следственных действий, направленных на поиск таких следов³².

Кроме того, в ст. 164 УПК РФ закреплены разнообразные возможности применения технических средств и способов агрегирования и изъятия электронно-цифровых следов. Правда, остаётся неурегулированным вопрос использования технических средств при производстве иных процессуальных действий (получение объяснений; проведение исследований³³, представление предметов и документов в электронном виде, задержание подозреваемого; получение устного заявления о преступлении и пр.).

В настоящее время криминалисты достаточно удачно справляются с задачами поиска, исследования и использования цифровых следов. Постоянно обобщается опыт раскрытия и расследования таких преступлений. Созданы и успешно работают экспертные подразделения по

²⁹ Семенов Г. В. Расследование преступлений в сфере мобильных телекоммуникаций: дис...канд. юрид. наук. Воронеж, 2003. С.148.

³⁰ Литвинов В. А. Программное обеспечение информационных технологий // Информационные технологии в юридической деятельности. СПб.: Питер, 2013. С. 59–110.

³¹ Букин М. С. Мобильник: друг и защитник или угроза свободе и кошельку. СПб.: БХВ-Петербург, 2005. С. 52.

³² Вехов В. Б. Особенности проведения доследственной проверки по делам о

преступлениях в сфере компьютерной информации // Эксперт-криминалист. 2013. № 4. С. 2–4. Поляков В. В. Особенности производства осмотра по компьютерным преступлениям // Российский следователь. 2017. № 21. С. 14–17.

³³ Ряполова Я. П. Исследования предметов и документов как новая форма использования специальных познаний в стадии возбуждения уголовного дела // Российский следователь. 2010. № 24. С. 2–5.

исследованию цифровых объектов. На вооружении правоохранительных органов имеются новейшие технические средства, которые позволяют успешно извлекать и

анализировать информацию, содержащуюся в компьютерах и сотовых телефонах. Работа практиков и учёных в этом направлении продолжается.

Список литературы

1. Блюменау Д. И. Информация и информационный сервис. Л.: Система, 1989. 188 с.
2. Борковский А. Б. Англо-русский словарь по программированию и информатике (с толкованиями): около 6000 терминов. М.: Московская международная школа переводчиков, 1992. 332 с.
3. Букин М. С. Мобильник: друг и защитник или угроза свободе и кошельку. СПб.: БХВ-Петербург, 2005. 239 с.
4. Вехов В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки. Волгоград: ВА МВД России, 2008. 401 с.
5. Жардев П. А. Методы и способы получения доказательственной информации с электронных носителей / П. А. Жардев, Ю. В. Шаров. Хабаровск. 2013. 88 с.
6. Карась И. З. Экономический и правовой режим информационных ресурсов // Право и информатика / под ред. Е. А. Суханова. М.: Изд-во МГУ, 1990. С. 40–59.
7. Козинкин В. А. Использование в расследовании преступлений информации, обнаруживаемой в средствах сотовых систем подвижной связи: автореф. дис. ... канд. юрид. наук. М., 2009. 26 с.
8. Литвинов В. А. Информационные технологии в юридической деятельности. СПб.: Питер, 2013. 320 с.
9. Правовая информатика и кибернетика: учебник / под ред. Н. С. Полевого. М.: Юридическая литература, 1993. 527 с.
10. Практические основы компьютерно-технической экспертизы / А. Б. Нехорошев [и др.]. Саратов: Научная книга, 2007. 264 с.
11. Ряполова Я. П. Исследования предметов и документов как новая форма использования специальных познаний в стадии возбуждения уголовного дела // Российский следователь. 2010. № 24. С. 2–5.
12. Семенов Г. В. Расследование преступлений в сфере мобильных телекоммуникаций: дис...канд. юрид. наук. Воронеж, 2003. 242 с.
13. Способы получения доказательств и информации в связи с обнаружением (возможностью обнаружения) электронных носителей: учебное пособие / В. Ф. Васюков, Б. Я. Гаврилов, А. А. Кузнецов [и др.]; под общ. ред. Б. Я. Гаврилова. М.: Проспект, 2017. 160 с.

14. Швоев М. И. Технология работы в компьютерных сетях // Информационные технологии в юридической деятельности. М.: Юрайт, 2013. 430 с.

15. Шурухнов Н. Г. Технология и процессуальный порядок выемки электронной почты (E-mail) при расследовании отдельных видов преступлений // Нюрнбергский процесс – приговор фашизму: материалы Международной науч.-практ. конференции в рамках праздничных мероприятий, посвященных 70-летию Победы в Великой Отечественной войне. 2015. С. 339–346.

16. Электронные носители информации в криминалистике: монография / И. В. Александров [и др.]; под ред. д-ра юрид. наук О. С. Кучина. Москва: Юрлитинформ, 2017. 300 с.

17. Электронные носители информации в криминалистике: монография/ И. В. Александров, Д. В. Бахтеев, В. Б. Вехов [и др.]. Москва: Издательство «Юрлитинформ», 2017. 304 с.

Nikolay V. Karepanov

PhD (Law), Associate Professor,
Associate Professor of the Department of Criminalistics,
Ural State Law University named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
karepanovvv@gmail.com

FEATURES OF THE TECHNOLOGY OF AGGREGATION, RESEARCH AND USE OF ELECTRONIC DIGITAL TRACES OF CRIME

Abstract: The article examines the issues of the essence, classification of electronic digital traces, features of their detection, research, and use. First, in the process of detecting and studying computer traces, not the information itself is extracted, but its external signs in the form of information that it contains. Modern knowledge about electronic traces is related to the content and structure of the concept of «information», the analysis of which is carried out in the first part of the article. The information contained in electronic traces can be recorded on any tangible medium and is manifested in the following terms: file, network address, domain name, electronic message, electronic document, information system, Internet site, internet site page, electronic signature, computer program (computer program), database, electronic journal, electronic money.

A storage medium is a physical medium that directly stores information. An information carrier is a strictly defined part of a particular information system that serves for intermediate storage or transmission of information.

The basis of modern information technology is a computer (PC). Storage media for it are external storage devices (external memory). They can be classified on various grounds, including the type of execution, the material of manufacture, etc.

The technology of searching, detecting, fixing, and seizing electronic evidence in computer devices is based on the features of data creation, storage and exchange using electronic devices.

To determine the search technology, it is necessary to know which provider the person whose e-mail is being detected is using. This can be done by identifying the phone number of the provider with which the subscriber is contacting. To access the provider's server, the subscriber can also use the phone numbers of relatives and friends.

Another way may be to obtain information from providers operating in the region where the person of interest to the searcher resides, whether there are servers of the electronic mailbox of a particular subject but owned by them.

Keywords: electronic-digital traces, storage medium, information technology, search technologies, provider, e-mail, server, electronic mailbox, integrated computer tool.

УДК 343.98

Нелюбин Константин Александрович

Кандидат юридических наук, старший следователь-криминалист
второго отдела криминалистического сопровождения следствия
Главного следственного управления Следственного комитета Российской
Федерации по Республике Крым и г. Севастополю
(г. Севастополь, Российская Федерация)
nelyubin.82@mail.ru

ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННОЙ БАЗЫ ДАННЫХ ПРИ РАССЛЕДОВАНИИ СЕРИЙНЫХ ПРЕСТУПЛЕНИЙ ПРОТИВ ПОЛОВОЙ СВОБОДЫ И НЕПРИКОСНОВЕННОСТИ

Аннотация: Статья посвящена вопросам создания и использования электронной базы данных преступлений против половой свободы и неприкосновенности личности. На примере раскрытия серийного преступления автор описывает структуру, функции электронной базы данных, которая должна содержать сведения не только о преступлениях, преступниках и потерпевших, но и о лицах, проверяемых на причастность к совершённым деяниям.

Ключевые слова: электронная база данных, преступления против половой свободы и неприкосновенности личности, серийные преступления, поступок как форма текста, выявление контекста.

Для цитирования:

Нелюбин К. А. Использование электронной базы данных при расследовании серийных преступлений против половой свободы и неприкосновенности // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 105–109.

В соответствии с концепцией учёного-экономиста Н. Д. Кондратьева, мы живём на излёте пятого технологического уклада. Е. Н. Каблов отмечает, что в 2020–2025 годах назревает новая научно-техническая и технологическая революция, основой которой станут разработки, синтезирующие достижения базовых направлений, в том числе искусственного интеллекта,

что, в конечном счёте, обеспечит выход на принципиально новый уровень в системах управления государством, обществом, экономикой¹. В определённой степени этот процесс затронул и криминалистику, что отмечают такие

¹ Каблов Е. Н. Шестой технологический уклад // Наука и жизнь. URL:

<https://www.nkj.ru/archive/articles/17800/> (дата обращения: 05.05.2022).

ученые как А. А. Бессонов², В. Ю. Толстолицкий³.

С 2009 по 2017 гг. – в период работы в следственном управлении Следственного комитета Российской Федерации по Свердловской области – нами разработана электронная база данных на основе криминалистической характеристики преступлений (далее – КХП) как основа для эффективного раскрытия и расследования убийств⁴.

В 2016–2021 гг. с учётом специфики преступности региона нами разработана аналогичная база данных для раскрытия и расследования преступлений против половой свободы и неприкосновенности личности, совершённых на территории города Севастополь.

База данных состоит из связанных между собой основных таблиц: «характеристики преступления», «характеристики жертвы», «характеристики преступника», «характеристики проверяемых на причастность лиц».

В содержание указанных таблиц помимо традиционных элементов криминалистической характеристики изнасилований и действий сексуального характера вошли, например, такие элементы, как фразы, которые произносил преступник во время нападения; сведения об облике потерпевших (внешности, предметах их одежды), с прикреплением фото

жертв, их одежды на момент нападения.

По первому элементу, например, выявлена серия преступлений, совершённых Я., представлявшимися своим малолетним жертвам врачом – 8 эпизодов нападений в отношении малолетних. По второму элементу выявлен типаж жертв, на которых нападал серийный насильник Т. – 17 эпизодов нападений в отношении малолетних детей, несовершеннолетних подростков и женщин. Сравнительный анализ совершённых Т. преступлений позволил достаточно точно спрогнозировать временные периоды и места его нападений, что способствовало установлению его личности.

Кроме того, анализ не только текстовых, но и визуальных сведений, позволил понять критерии выбора преступником своих жертв, которых можно разделить по двум группам:

- подростки и женщины 14–26 лет, невысокого роста (около 160 см), худощавого телосложения, одетые в пуховики ярких расцветок (белые, красные, розовые, зелёные) или имеющие иные предметы одежды, бросающиеся в глаза (например, жёлтая шапка с помпоном). Все указанные потерпевшие в вечернее время возвращались домой от остановок транспорта.

² Бессонов А. А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений: моногр. М.: Проспект, 2021. 816 с.

³ Толстолицкий В. Ю., Кузенкова В. Г. Обучение выдвижению версий на криминалистическом полигоне с помощью

компьютерной программы «Форвер» // International Journal of Open Information Technologies. 2014. Т. 2, № 1. С. 24–31.

⁴ Нелюбин К. А. Программирование и алгоритмизация установления лица, совершившего убийство: моногр. М.: Юрлитинформ, 2018. 152 с.

- дети возраста 8–10 лет. Все потерпевшие данной группы гуляли во дворах своих домов.

В зависимости от группы потерпевших и обстановки нападения, преступник выбирал различный способ подготовки и совершения преступления, сокрытия следов. В отношении потерпевших первой группы он заблаговременно прибывал к месту наблюдения за остановкой транспорта. После выхода потерпевшей из транспорта выслеживал её до определённого места, нападал сзади, совершал изнасилование или насильственные действия сексуального характера, скрывая своё лицо, после чего покидал место преступления. Из анализа вышеуказанных сведений о потерпевших стало очевидно, что преступник выбирал объект нападения не по возрасту, а по параметрам внешности. Во второй группе потерпевших его, напротив, интересовал возраст, а не внешность детей. Им он демонстрировал свои половые органы, занимался мастурбацией в их присутствии, таким образом доказывая свою мужскую состоятельность.

Очевидно, что получить указанные сведения только из материалов уголовных дел практически невозможно, поскольку тексты протоколов следственных действий, даже с приложением фототаблиц, зачастую не содержат необходимой информации. Эту информацию необходимо собирать не по результатам расследования, а

непосредственно во время его проведения, что стало понятным в ходе формирования электронной базы данных.

Методологически, в этом смысле, мы стоим на позиции, которую выразил М. М. Бахтин, считавший, что человеческий поступок есть потенциальный текст и может быть понят (как человеческий поступок, а не физическое действие) только в диалогическом контексте своего времени (как реплика, как смысловая позиция, как система мотивов)⁵. Понимать же такой текст необходимо по формуле Ф. Шлейермахера: «сначала наравне с автором, а потом и превзойти его. Стремиться осознать многое из того, что он не осознавал сам, исключая те случаи, когда он, рефлексировав, становится своим собственным читателем»⁶.

Электронная база данных, таким образом, стала накопителем той контекстной информации, которая позволила глубже понять личность преступника, предвосхитить его поведение, и, в результате, установить его личность.

При формировании базы данных в качестве её структурных элементов сформирована отдельная таблица лиц, проверяемых на причастность, с её собственными подэлементами:

- лица, ранее судимые за совершение аналогичных преступлений;
- лица, проходившие фигурантами по материалам проверок о действиях сексуального характера;

⁵ Бахтин М. М. Эстетика словесного творчества. М.: Искусство, 1979. С. 286.

⁶ Шлейермахер Ф. Герменевтика. С.-Петербург: Европейский дом, 2004. С. 64.

- лица, состоящие на психиатрическом / наркологическом учёте;
- лица, доставлявшиеся в отделы полиции по различным основаниям;
- лица, привлечённые к административной ответственности в периоды, непосредственно следующие за датой нападения;
- абоненты, чьи телефоны работали в районе нападения на потерпевших;
- собственники транспорта, который попал в выборку камер ГИБДД «Поток» по маршрутам, проходящим вблизи мест нападения;
- лица, допрошенные, опрошенные по делам, материалам проверок;
- лица, у которых отобраны образцы буккального эпителия (результат их проверки по учёту ДНК).

Ведение такой таблицы позволило собрать большой объём информации и оперативно определять организационные пробелы в расследовании, которые необходимо устранять для раскрытия преступления. Благодаря такой работе в процессе расследования серии преступлений против половой неприкосновенности несовершеннолетних и половой свободы женщин, совершённых Т. на территории города Севастополь и Республики Крым, были раскрыты более 30 иных преступлений, в том числе носящих серийный характер.

Особенно важно, что с учётом собранных данных, информация в базе данных сохранила свою актуальность и после раскрытия преступлений. Задача состоит только в том, чтобы регулярно актуализировать содержащуюся в базе данных информацию в связи с вновь совершаемыми преступлениями.

Список литературы

1. Бахтин М. М. Эстетика словесного творчества. / сост. С. Г. Бочаров, примеч. С. С. Аверинцев, С. Г. Бочаров. М.: Искусство, 1979. 423 с.
2. Бессонов А. А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений: моногр. М.: Проспект, 2021. 816 с.
3. Каблов Е. Н. Шестой технологический уклад // Наука и жизнь. URL: <https://www.nkj.ru/archive/articles/17800/>.
4. Нелюбин К. А. Программирование и алгоритмизация установления лица, совершившего убийство: моногр. М.: Юрлитинформ, 2018. 152 с.
5. Толстоуцкий В. Ю. Обучение выдвижению версий на криминалистическом полигоне с помощью компьютерной программы «Форвер» / В. Ю. Толстоуцкий, В. Г. Кузенкова // International Journal of Open Information Technologies. 2014. Т. 2, № 1. С. 24–31.
6. Шлейермахер Ф. Герменевтика / пер. с немецкого А. Л. Вольского. С-Петербург, «Европейский дом», 2004. 242 с.

Konstantin A. Nelyubin

PhD (Law), Senior investigator-criminalist
of the second department of forensic support of the investigation
of the Main Investigative Department of the Investigative Committee of the Russian
Federation for the Republic of Crimea and Sevastopol
(Sevastopol, Russian Federation)
nelyubin.82@mail.ru

THE USE OF AN ELECTRONIC DATABASE IN THE INVESTIGATION OF SERIAL CRIMES AGAINST SEXUAL FREEDOM AND INVIOABILITY

Abstract: The article is devoted to the creation and use of an electronic database of crimes against sexual freedom and personal integrity. Using the example of the disclosure of a serial crime, the author reveals the structure and functions of an electronic database, which should contain information not only about crimes, criminals and victims, but also about persons being checked for involvement in committed crimes.

Keywords: electronic database, crimes against sexual freedom and personal integrity, serial crimes, an act as a form of text, identification of context.

Олифиренко Екатерина Павловна

Кандидат политических наук,
доцент кафедры уголовного права и процесса,
Северо-Кавказская государственная академия
(г. Черкесск, Российская Федерация)
anna-54@bk.ru

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ОРГАНОВ ПРОКУРАТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация: В научной статье исследуются проблемы информационного обеспечения прокурорской деятельности в условиях развития цифровой экономики Российской Федерации. На основе анализа действующего законодательства автором предлагаются практические решения существующих проблем, направленные на улучшение обмена информацией между территориальными прокуратурами и совершенствование межведомственного взаимодействия.

Ключевые слова: прокуратура, прокурорский надзор, информация, цифровизация, информационные технологии, информационная безопасность.

Для цитирования:

Олифиренко Е. П. Актуальные проблемы информационного обеспечения органов прокуратуры Российской Федерации // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 110–115.

Активное использование информационных технологий во всех сферах профессиональной деятельности государственных органов становится неотъемлемой частью жизни современного общества. Безусловно, тенденции постепенной цифровизации затронули и правоохранительную систему, в том числе органы прокуратуры¹. Внедрение информационно-телекоммуникационных систем при

осуществлении прокурорской деятельности рассматривается в качестве одного из значимых компонентов её оптимизации в вопросах прогнозирования оперативной обстановки, своевременного реагирования на правонарушения, планирования работы управленческих структур и служб, а также оценки результативности функционирования подразделений².

¹ Авдеева Е. В., Гордей В. А. Оптимизация правоприменения в условиях внедрения информационно-коммуникационных

технологий // Право и законодательство. 2018. № 10. С. 94.

² Колесов М. В. О некоторых путях оптимизации деятельности

Осуществляя свою деятельность в различных областях, прокуратура взаимодействует с другими правоохранительными органами по вопросам сбора и обработки информации, что выступает отправной точкой в процессе создания, развития и внедрения информационных систем в органах и организациях прокуратуры Российской Федерации.

Цифровая трансформация органов и организаций прокуратуры осуществляется в рамках государственной политики по созданию необходимых условий для развития цифровой экономики Российской Федерации. Однако стоит отметить, что действующее российское законодательство не содержит чёткого определения цифровой трансформации – общее современное понимание данного процесса даёт изучение и анализ ряда нормативно-правовых актов, в том числе ведомственного характера.

Так, Указом Президента Российской Федерации от 21.07.2020 № 474 определены основные национальные цели развития Российской Федерации на период до 2030 года и одним из приоритетных направлений обозначена цифровая трансформация³. Для обеспечения эффективной работы прокурора в современной цифровой среде

совместным Приказом от 8 февраля 2018 г. № 68/56 Генеральной прокуратуры РФ и Министерства связи и массовых коммуникаций РФ был утверждён паспорт проекта цифровой трансформации органов и организаций прокуратуры⁴.

Мероприятия по цифровой трансформации органов и организаций прокуратуры включены в федеральный проект «Цифровое государственное управление» национальной программы «Цифровая экономика Российской Федерации». В рамках пилотного проекта, реализуемого с 2017 года, запланированы и почти полностью успешно реализованы мероприятия по осуществлению цифровизации органов прокуратуры в следующих направлениях:

- повышение эффективности деятельности органов прокуратуры по обеспечению законности и правопорядка;
- подготовка и создание условий для оперативной реализации надзорной функции в отношении объектов, подвергнутых цифровизации;
- создание условий для устойчивого и бесперебойного функционирования цифровой инфраструктуры органов прокуратуры, с учётом состояния

правоохранительных органов по сбору и обобщению. Статистическая информация // Российский юридический журнал. 2017. № 3 (12). С. 29.

³ Указ Президента Российской Федерации от 21.07.2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года» // Официальный сайт Президента РФ. URL: [http://](http://www.kremlin.ru/acts/bank/45726)

www.kremlin.ru/acts/bank/45726 (дата обращения: 05.05.2022).

⁴ Приказ №68/56 «Об утверждении паспорта проекта цифровой трансформации органов и организаций прокуратуры Российской Федерации» // Генеральная прокуратура РФ: официальный сайт. URL: <https://epp.genproc.gov.ru/web/gprf/documents?item=1730643> (дата обращения: 08.05.2022).

информационной безопасности, степени её угроз;

- реализация плавного перехода к сервисной модели цифровой инфраструктуры органов прокуратуры и её постепенное развитие;

- обеспечение безопасных условий для свободного и устойчивого взаимодействия органов прокуратуры с гражданами, организациями, институтами гражданского общества, органами государственной власти, местного самоуправления⁵.

Необходимо отметить, что прокуратура, осуществляя координацию деятельности правоохранительных органов, а также надзор за исполнением законов участниками данной деятельности, активно осуществляет мероприятия в рамках Концепции цифровой трансформации органов и организаций прокуратуры Российской Федерации до 2025 года⁶. Во многом связанные с совершенствованием действующих систем и внедрением перспективных информационных технологий, в Концепции обозначены основные приоритеты информационного обеспечения органов прокуратуры и принципы его развития в рамках государственной политики по

созданию необходимых условий для развития цифровой экономики⁷.

Следует признать, что в настоящий момент ведётся активная разработка соответствующей методическо-технологической базы по приоритетным направлениям развития инфраструктуры в рамках реализации цифровой трансформации в органах прокуратуры, а именно:

- апробирован запуск защищённой сети передачи данных органов прокуратуры посредством создания защищённого интернета для органов государственной власти через сегмент сети Интернет, а также создание аттестованной единой защищённой сети передачи данных для каждого рабочего места работника прокуратуры;

- организована единая система защищённых автоматизированных рабочих мест для сотрудников органов прокуратуры, в том числе с возможностью использования защищённой электронной почты с настройкой для каждого сотрудника;

- осуществлён переход с фиксированной телефонной связи на IP-телефонию с возможностью организации видеозвонков и аудиоконференций;

⁵ Яцуценко В. В. Проблемы и перспективы внедрения цифровых технологий в деятельность органов прокуратуры // Актуальные проблемы российского права. 2021. Т. 16, № 11. С. 191

⁶ Приказ Генерального прокурора Российской Федерации от 21 сентября 2017 г. № 627 «Об утверждении Концепция цифровой трансформации органов и организаций прокуратуры до 2025 года». // Генеральная прокуратура РФ: официальный сайт. URL:

<http://genproc.gov.ru/documents/orders/627> (дата обращения: 08.05.2022).

⁷ Кореньюк А. Л. Некоторые вопросы обеспечения информационной безопасности в органах прокуратуры Российской Федерации в условиях цифровой трансформации // Цифровизация деятельности органов прокуратуры: сб. материалов семинара (круглого стола) (Москва, 30 сентября 2020 г.) / Ун-т прокуратуры Российской Федерации. М., 2021. С. 98.

- проведена установка систем видеоконференцсвязи в органах прокуратуры всех субъектов;
- начался переход на электронный документооборот, в ряде субъектов введены в действие пилотные проекты по его внедрению;
- в отдельных прокуратурах реализован пилотный проект по отработке процедур сбора и учёта статистической информации исключительно в электронном виде;
- введён в опытную эксплуатацию модуль «Учёт работы прокурора» на 3 200 рабочих местах;
- введён в эксплуатацию Единый портал органов прокуратуры с функционалом аккредитации средств массовой информации; обеспечен и успешно функционирует автоматизированный мониторинг СМИ и сети «Интернет»;
- проведены и успешно реализуются программы обучения работников органов прокуратуры в рамках цифровой трансформации и ряд других мероприятий.

По данным официального сайта Генеральной прокуратуры в рамках продолжающейся в 2021 году цифровой трансформации органов прокуратуры, направленной в том числе на повышение эффективности надзора, органам прокуратуры удалось достичь конкретных результатов по активизации межведомственного электронного взаимодействия. Так, для автоматизации различных

направлений деятельности органов прокуратуры разработаны и применяются 12 информационных систем и комплексов, среди которых активно используется информационная система межведомственного электронного взаимодействия Генеральной прокуратуры Российской Федерации. Вследствие внедрения обозначенных информационных систем получена возможность информационного взаимодействия с Федеральной налоговой службой, Росреестром, МВД России, МЧС России, Минцифры России, Федеральным казначейством, Пенсионным фондом Российской Федерации, Федеральной службой по финансовому мониторингу, Федеральным агентством лесного хозяйства⁸.

На сегодняшний день Генеральной прокуратурой Российской Федерации ведётся работа по реализации комплекса мероприятий, направленных на модернизацию программного обеспечения, увеличение перечня получаемых сведений, повышение отказоустойчивости системы, создание электронных сервисов, по которым требуется передавать ответы в соответствующие органы. Также с 1 июля 2021 года введена в промышленную эксплуатацию федеральная государственная информационная система «Единый реестр контрольных (надзорных) мероприятий», формирование и

⁸ В рамках продолжающейся цифровой трансформации органами прокуратуры активизировано межведомственное электронное взаимодействие. 24 мая 2021 // Цифровая трансформация органов

прокуратуры. Генеральная прокуратура Российской Федерации: официальный сайт. URL: https://epp.genproc.gov.ru/web/gprf/expert_advice/news (дата обращения: 03.05.2022).

ведение которой предусмотрено Федеральным законом от 31 июля 2020 года № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации». Данная система обеспечивает информационное взаимодействие контрольных (надзорных) органов и органов прокуратуры Российской Федерации в рамках планирования и согласования проведения контрольных (надзорных) мероприятий, а также позволяет автоматизировать учёт иных мероприятий, в том числе профилактических, специальных режимов государственного контроля (надзора), принятых мер по пресечению нарушений обязательных требований, устранению их последствий. На сегодняшний день в числе пользователей системы – 2 405 прокурорских работников и 32 168 уполномоченных должностных лиц контрольных (надзорных) органов.

В условиях информационного общества цифровое использование означает реализацию новых типов инноваций в конкретной области, а не только усиление и поддержку традиционных методов работы, однако применительно к правоохранительной деятельности понятие «цифровой трансформации», как правило, сводится к безбумажному обращению.

В этом ключе в основном и выполнены анализируемые российские нормативные документы. Так, при разработке Концепции основной упор делается на «развитие цифровой инфраструктуры на основе применения российских информационно-телекоммуникационных технологий», вместе с тем решение обозначенной проблемы в силу определённых обстоятельств может потребовать дальнейшего совершенствования действующего законодательства.

Решение рассматриваемых проблем по обеспечению цифровой трансформации органов прокуратуры должно осуществляться в рамках создания среды электронного взаимодействия с учётом потребностей граждан, общества и государственных органов в получении качественных и достоверных сведений. Развитие сетевых технологий в органах прокуратуры определяется и внедрением новых средств защиты информации, предназначенных для обеспечения безопасности взаимодействия с другими автоматизированными системами и внешними сетями для защиты информации от вмешательства нарушителей.

Список литературы

1. Авдеева Е. В. Оптимизация правоприменения в условиях внедрения информационно-коммуникационных технологий / Е. В. Авдеева, В. А. Гордей // Право и законодательство. 2018. № 10.
2. В рамках продолжающейся цифровой трансформации органами прокуратуры активизировано межведомственное электронное взаимодействие // Цифровая трансформация органов прокуратуры. Генеральная прокуратура

Российской Федерации: официальный сайт. 2021. 24 мая. URL: https://epp.genproc.gov.ru/web/gprf/expert_advice/news.

3. Колесов М. В. О некоторых путях оптимизации деятельности правоохранительных органов по сбору и обобщению. Статистическая информация // Российский юридический журнал. 2017. № 3 (12). С. 235–239.

4. Коренюк А. Л. Некоторые вопросы обеспечения информационной безопасности в органах прокуратуры Российской Федерации в условиях цифровой трансформации // Цифровизация деятельности органов прокуратуры: сб. материалов семинара (круглого стола) (Москва, 30 сентября 2020 г.) / Ун-т прокуратуры Российской Федерации. М., 2021.

5. Яцуценко В. В. Проблемы и перспективы внедрения цифровых технологий в деятельность органов прокуратуры // Актуальные проблемы российского права. 2021. Т. 16, № 11. С. 187–193.

Ekaterina P. Olifirenko

PhD (Political Sciences),

Associate Professor of the Department of Criminal Law and Procedure,
North Caucasus State Academy
(Cherkessk, Russian Federation)
anna-54@bk.ru

ACTUAL PROBLEMS OF INFORMATION SUPPORT OF THE PROSECUTOR'S OFFICE OF THE RUSSIAN FEDERATION

Abstract: The scientific article examines the problems of information support of prosecutorial activity in the context of the development of the digital economy of the Russian Federation. Based on the analysis of the current legislation, the author offers practical solutions to existing problems related to improving the exchange of information between territorial prosecutor's offices and improving interdepartmental interaction.

Keywords: prosecutor's office, prosecutor's supervision, organization of prosecutorial activity, information, digitalization, information technology, information security.

Титов Павел Михайлович

Кандидат юридических наук, преподаватель кафедры уголовного процесса,
Уральский юридический институт МВД России
(Екатеринбург, Российская Федерация)
titov1995@ya.ru

К ВОПРОСУ О НАЧАЛЕ УГОЛОВНОГО ПРЕСЛЕДОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННОЙ СРЕДЫ

Аннотация: Статья посвящена вопросам уголовного преследования по уголовно-процессуальному законодательству Российской Федерации с использованием электронной среды. Анализируются законодательные нормы, регламентирующие уголовное преследование, теоретическое осмысление данного вопроса, а также практическое применение норм, посвященных уголовному преследованию.

Ключевые слова: уголовный процесс, уголовно-процессуальное право, уголовное преследование, процессуальные отношения, электронные технологии, электронное заявление.

Для цитирования:

Титов П. М. К вопросу о начале уголовного преследования с использованием электронной среды // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 116–120.

Понятие «уголовное преследование» является одним из наиболее важных в уголовно-процессуальном праве. В настоящее время оно сформулировано на нормативном уровне. Уголовно-процессуальный кодекс Российской Федерации¹ (далее – УПК РФ) определяет уголовное преследование как процессуальную деятельность, осуществляемую стороной обвинения в целях изобличения подозреваемого, обвиняемого в совершении преступления п. 55 ст. 5 УПК РФ.

Обращает на себя взор законодательная формулировка, которая является краткой и не отражает все существенные признаки данного явления. Учитывая это, специалисты в области уголовного процесса предлагают более полную дефиницию уголовного преследования. М. С. Строгович полагает, что «уголовное преследование – это обвинение как процессуальная функция, т. е. обвинительная деятельность, которая состоит в формировании

¹ Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-

ФЗ // Собрание законодательства РФ. 2001. № 52 (ч.1). Ст. 4921.

обоснованного вывода о совершении определенным лицом конкретного общественно опасного деяния, предусмотренного уголовным законом»². При этом, Ю. В. Козубенко вносит определенное дополнение и подчеркивает, что «уголовное преследование – это движущая сила уголовного процесса»³. Определение В. Ю. Стельмаха наиболее глубинно отражает существенные признаки уголовного преследования и разделяется автором в полной мере: «Уголовное преследование – публичная, государственно-властная деятельность, составляющая основное содержание уголовного судопроизводства, осуществляемая официальными государственными органами и должностными лицами при ограниченном участии других участников уголовного процесса, в формах и порядке, предусмотренном уголовно-процессуальным законом, направленная на установление лица, совершившего преступление, предъявление ему обвинения и обоснование данного обвинения перед судом»⁴. П. М. Титов выделял некоторые проблемы уголовного преследования в рамках дел частного обвинения, показывая особенности его осуществления по данной категории уголовных дел⁵.

Как можем увидеть из вышесказанного, ученые-

процессуалисты в своих работах трактуют данное понятие по-разному, хотя и сохраняя при этом ключевые аспекты данного определения. При этом, никто из авторов не поднимает вопроса о начале уголовного преследования с использованием электронной среды.

В настоящее время имеются предпосылки к поэтапному переходу к электронному уголовному делу. Однако, до полноценного осуществления расследования по электронному уголовному делу еще далеко. Разбираясь в вопросах, связанных с начальным моментом, т. е. с уголовным преследованием, необходимо первоначально понять, с какого именно момента оно начинается, так как из законодательно закрепленной в УПК РФ формулировки не совсем понятно.

Можно сказать о двух позициях, сложившихся в уголовно-процессуальной теории. Первая позиция подразумевает в себе то, что уголовное преследование означает деятельность по изобличению конкретного лица, в том числе и наступление для него неблагоприятных последствий в виде задержания по подозрению в совершении преступления, привлечении в качестве обвиняемого, применении меры пресечения и т. п.

² Строгович М.С. Курс советского уголовного процесса. Т. 1. М., 1968. С. 194.

³ Козубенко Ю. В. Уголовное преследование как элемент механизма уголовно-правового регулирования // Государство и право. 2008. № 2. С. 109.

⁴ Стельмах В. Ю. Понятие и признаки уголовного преследования // Актуальные

проблемы борьбы с преступлениями и иными правонарушениями. 2014. № 14-1. С. 169–170.

⁵ Титов П. М. Некоторые проблемы уголовного судопроизводства по делам частного обвинения // Российский юридический журнал. 2019. № 4 (127). С. 69–77.

Вторая позиция состоит в том, что уголовное преследование – это деятельность по установлению причастного к совершению преступления лица, и лишь после этого по его привлечению к уголовной ответственности. Приверженцем данной позиции является А. Р. Белкин⁶.

В соответствии с позицией Конституционного Суда Российской Федерации «уголовное преследование начинается с момента возбуждения уголовного дела, поскольку с этого времени создаются правовые основания для последующих процессуальных действий органов дознания, предварительного следствия и суда»⁷. В другом постановлении Конституционный Суд Российской Федерации указал, что «любая деятельность органов предварительного расследования и прокуратуры, фактически направленная на выявление фактов и обстоятельств, уличающих лицо в совершении преступления, представляет собой уголовное преследование»⁸.

Таким образом, В. Ю. Стельмах выделял, что «Конституционный Суд

Российской Федерации не связывает момент начала уголовного преследования с установлением конкретного лица, которому придан процессуальный статус подозреваемого или обвиняемого»⁹.

На основании вышесказанного можно сделать вывод, что уголовное преследование содержит в себе два этапа, которые возможно осуществлять как в привычном варианте, так и с использованием электронной среды:

1. Неперсонифицированный. На этом этапе происходит деятельность, направленная на установление лица, совершившего преступление. Это же является главной задачей, так как на этом этапе конкретное лицо, подлежащее наделению процессуальным статусом подозреваемого или обвиняемого, еще не установлено, однако осуществляется активная деятельность органов предварительного расследования по собиранию доказательств, в том числе проводится комплекс мероприятий оперативного характера, материалы которых будут иметь процессуальный характер,

⁶ Белкин А. Р. Теория доказывания в уголовном судопроизводстве. М.: Норма, 2005. 226 с.

⁷ Постановление Конституционного Суда от 14 января 2000 года № 1-П «По делу о проверке конституционности отдельных положений Уголовно-процессуального кодекса РСФСР, регулирующих полномочия суда по возбуждению уголовного дела, в связи с жалобой гражданки И. П. Смирновой и запросом Верховного Суда Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_25945 (дата обращения: 10.05.2022).

⁸ Постановление Конституционного Суда от 27 июня 2000 года № 11-П «По делу о проверке конституционности положений части первой статьи 47 и части второй статьи 51 Уголовно-процессуального кодекса РСФСР в связи с жалобой гражданина В. И. Маслова» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_27705 (дата обращения: 10.05.2022).

⁹ Стельмах В. Ю. Понятие и признаки уголовного преследования // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2014. № 14-1. С. 169.

делающих возможным официальное утверждение о причастности определенного лица к совершению преступления. Данная деятельность не является «нейтральной» по отношению к уголовному преследованию, она органически входит в его содержание и создает необходимые предпосылки для перехода к персонифицированному этапу уголовного преследования.

Уголовно-процессуальная деятельность на указанном этапе совершается путем производства следственных и иных процессуальных действий, в результате которых собираются необходимые доказательства. Однако на неперсонифицированном этапе уголовного преследования не производится задержание лица в качестве подозреваемого и избрание мер пресечения.

2. Персонифицированный (обвинительная деятельность). Начало: с момента установления основания для придания лицу одного из процессуальных статусов – подозреваемого или обвиняемого.

Ряд ученых считает, что данного этапа вообще не существует и имеется только персонифицированный. Но определенная фаза, даже в ряде случаев ее можно назвать активной фазой, например, при проведении освидетельствования, по сбору и закреплению доказательств, начинается именно с момента сообщения о противоправном деянии

(принятие заявления, осмотр места происшествия, установление очевидцев и «круга» заподозренных). Что же касается дел частного обвинения, то по этим делам вообще нет подозреваемого, поскольку заявление подается мировому судье и уголовное дело не возбуждается в обычном понимании этого термина. Вместе с тем надо сказать, что частное обвинение в наше время не предусматривает неперсонифицированного этапа, поскольку, если личность виновного потерпевшему неизвестна, мировой судья не принимает заявление, а направляет его для возбуждения уголовного дела в общем порядке. Однако эта конструкция является исключением из правил и вызвана только спецификой производства по категории дел частного обвинения. Теоретически потерпевший мог бы и сам искать виновного, но тогда государство устранилось бы от выполнения правоохранительной функции, что в условиях демократии невозможно.

Уголовное преследование может быть начато и минуя неперсонифицированный этап, в случаях, когда идет раскрытие преступления во всех случаях, когда это происходит по схеме «от лица к преступлению». Примером может служить ситуация, когда лицо заявляет о совершенном им преступлении, то уголовное преследование начинается персонифицировано.

Список литературы

1. Белкин А. Р. Теория доказывания в уголовном судопроизводстве. М.: Норма, 2005. 527 с.

2. Козубенко Ю. В. Уголовное преследование как элемент механизма уголовно-правового регулирования // Государство и право. 2008. № 2. С. 108–113.
3. Стельмах В. Ю. Понятие и признаки уголовного преследования // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2014. № 14-1. С. 168–170.
4. Строгович М. С. Курс советского уголовного процесса. Т. 1. М., 1968. 470 с.
5. Титов П. М. Некоторые проблемы уголовного судопроизводства по делам частного обвинения // Российский юридический журнал. 2019. № 4 (127). С. 69–77.

Pavel M. Titov

PhD (Law), Lecturer of the Department of Criminal Procedure,
Ural Law Institute of the Ministry of Internal Affairs of the Russian Federation
(Yekaterinburg Russian Federation)
titov1995@ya.ru

TO THE QUESTION OF INITIATION OF CRIMINAL PROSECUTION USING THE ELECTRONIC ENVIRONMENT

Abstract: The article is devoted to the issues of criminal prosecution under the criminal procedure legislation of the Russian Federation using an electronic environment. Legislative norms governing criminal prosecution, theoretical understanding of this issue, as well as the practical application of norms devoted to criminal prosecution are analyzed.
Keywords: criminal process, criminal procedure law, criminal prosecution, procedural relations, electronic technologies, electronic statement.

УДК 343.98

Шишкина Елена Викторовна

Кандидат юридических наук, доцент,

доцент кафедры криминалистики,

Уральский государственный юридический университет

имени В. Ф. Яковлева

(г. Екатеринбург, Российская Федерация)

evsh18@mail.ru

НЕКОТОРЫЕ АСПЕКТЫ ПРОВЕДЕНИЯ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ С ИСПОЛЬЗОВАНИЕМ ВИДЕОКОНФЕРЕНЦСВЯЗИ

Аннотация: В статье рассмотрены отдельные проблемы, которые могут возникнуть при проведении допросов, очных ставок и предъявления для опознания с применением технологий видеоконференцсвязи. Сделан вывод о необходимости разработки тактико-криминалистического обеспечения следственных действий, проводимых с применением данного вида технологий, включающего в себя вопросы принятия решения о проведении следственного действия, организацию подготовки и взаимодействия с участниками, тактические приёмы и рекомендации по оформлению и фиксации его результатов.

Ключевые слова: следственные действия, видеоконференцсвязь, ВКС, тактико-криминалистическое обеспечение, взаимодействие.

Для цитирования:

Шишкина Е. В. Некоторые аспекты проведения следственных действий с использованием видеоконференцсвязи // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 121–128.

Изменения уголовно-процессуального законодательства в части правил проведения отдельных следственных действий с применением видеоконференцсвязи (далее – ВКС), о необходимости которых ранее писали многие, потребуют разработки актуальных тактических средств их сопровождения.

До этого момента уголовно-процессуальное законодательство предусматривало возможности использования ВКС только на судебных стадиях и в основном в целях

обеспечения оперативности судопроизводства, снижения расходов на этапирование заключённых из удалённых территорий, а также минимизации связанных с этим рисков (побеги, нападения и пр.). Ещё более актуальными стали эти технологии в период распространения коронавирусной инфекции, когда возникла необходимость максимально сократить контакты между людьми, в том числе и при посещении судебных органов.

Опыт применения этих технологий судами имеет неоднозначные оценки учёных, занимающихся их изучением. В целях реализации технических нововведений с 2000 года по всей стране началось формирование федеральной системы видеоконференцсвязи в Верховном Суде Российской Федерации (далее – ВС РФ). Отделом правовой информатизации ВС РФ были разработаны учебные программы, методические рекомендации и инструкции, проводятся курсы повышения квалификации сотрудников судов общей юрисдикции, следственных изоляторов, исправительных учреждений ФСИН России. Для реализации названных и иных проблем разработана Федеральная целевая программа «Развитие судебной системы России» на 2007–2011 годы¹. В то же время несмотря на в целом положительную оценку этих нововведений, многие отмечают наличие технических сложностей, с которыми столкнулись суды. В частности, П. А. Устинкин пишет, что «технические средства связи, которые при этом используются, оставляют желать лучшего: постоянные обрывы, плохая слышимость и иные сопутствующие технические сбои вряд ли способствуют проведению того или

иного следственного действия в нормальных условиях без потери качества»².

Тем не менее, опыт применения технологий ВКС в судебных стадиях уже накоплен и в какой-то степени может быть использован при их реализации в досудебном производстве.

Помимо технических проблем реализации этих новелл, безусловно, возникнут проблемы с их организационным и тактическим обеспечением. Из ч. 2 ст. 189.1 УПК РФ вытекает, что у следователя и дознавателя теперь появились новые полномочия – давать письменные поручения об организации проведения следственных действий, перечисленных в данной статье. Следователь теперь имеет право давать такие поручения другому следователю и дознавателю, а дознаватель – другому дознавателю, расположенным по месту нахождения участника следственного действия. Это предполагает внедрение новых форм взаимодействия между указанными должностными лицами. Кроме того, на следователя (дознавателя), получившего такое поручение, возлагается обязанность по организации следственного действия посредством ВКС, что требует решения большого числа вопросов,

¹ Новикова Ю. В. Проблемы и перспективы применения видеоконференц-связи в уголовном процессе // Актуальные проблемы деятельности подразделений УИС : Сборник материалов открытой Всероссийской научно-практической конференции, в 2-х т. (Воронеж, 25 мая 2011 года). Воронеж: Воронежский институт ФСИН России, 2011. С. 377–378.

² Устинкин П. А. Допрос с использованием систем видео-конференц-связи // Актуальные проблемы борьбы с преступностью: вопросы теории и практики: Материалы XXV международной научно-практической конференции. В 2-х частях (Красноярск, 07–08 августа 2022 года) / отв. ред. Д. В. Ким. Красноярск: Сибирский юридический институт Министерства внутренних дел Российской Федерации, 2022. С. 150.

напрямую не урегулированных законом: обеспечение явки на следственное действие, подбор статистов и понятых для проведения предъявления для опознания, — а также ряда вопросов тактического характера, закономерно возникающих на начальной стадии следственного действия, включая установление контакта, снятие напряжённости, разъяснение смысла происходящего. Поскольку закон фактически допускает участие в этих следственных действиях лиц любого процессуального статуса, в том числе обладающих специфическими особенностями, требующими особых правил проведения следственного действия, то круг обязанностей, вытекающих из письменного поручения, возрастает ещё больше. Если участник следственного действия несовершеннолетний, и к тому же страдает психическим расстройством или отстаёт в психическом развитии, то к допросу (или иному следственному действию с его участием) могут быть привлечены законный представитель, психолог или педагог. В других ситуациях может возникнуть необходимость приглашения защитника, переводчика.

В законе нет упоминания о сроках исполнения письменного поручения следователем

(дознавателем). Согласимся с К. С. Плахота, что «отсутствие четко ограниченных временных рамок при производстве следственного действия дистанционно сводит его эффективность к нулю и лишает преимуществ перед обычным поручением о проведении, например, допроса свидетеля иными должностными лицами»³.

В число следственных действий, которые могут быть проведены согласно ст. 189.1 УПК РФ в режиме ВКС, законодатель включил допрос, очную ставку и предъявление для опознания. Ранее суды могли с помощью ВКС проводить только допросы, опыта проведения других следственных действий с применением этих технологий нет. При этом многие авторы полагают, что в перечень следственных действий, которые могут осуществляться по новым правилам, следовало включить и освидетельствование⁴.

Одной из проблем, которые, возможно, возникнут при проведении допросов с применением ВКС, называют ограниченную возможность следователя (дознавателя), ведущего расследование, наблюдать за всем происходящим в месте производства допроса. К. С. Плахота приводит пример недобросовестного ведения допроса, при котором на

³ Плахота К. С. Использование следователем (дознавателем) видео-конференц-связи при производстве следственных действий // Известия Тульского государственного университета. Экономические и юридические науки. 2022. № 1. С. 97.

⁴ См., например: Кравец Е. Г., Шувалов Н. В., Мартынов А. Н. Перспективы использования видеоконференц-связи при производстве

следственных действий на досудебных стадиях уголовного судопроизводства // Юридическая наука и правоохранительная практика. 2017. № 4 (42). С. 180–181; Арсенова Н. В., Орлова Е. А. Перспективы применения видеоконференцсвязи в досудебном производстве // Вестник Барнаульского юридического института МВД России. 2020. № 1 (38). С. 136.

допрашиваемое лицо было оказано давление с целью получения «нужных» показаний. Она же предлагает во избежание подобных ситуаций производить видеосъёмку помещения, где проводится допрос с двух точек с целью охвата всего пространства⁵.

На наш взгляд, больше проблем, связанных с допросом в режиме ВКС, может возникнуть в случаях его проведения в условиях конфликтных ситуаций. Эти ситуации требуют активного тактического воздействия на допрашиваемое лицо, использования многочисленных тактических приёмов и их комбинаций, для эффективности которых большое значение имеет анализ следователем психологических реакций допрашиваемого на поставленные вопросы и предъявленные ему доказательства. Особенности восприятия реакций, поведения человека через экран значительно снижают эти возможности, а значит, могут повлиять на эффективность допроса. Всё это позволяет прийти к выводу, что допросы в режиме ВКС следует проводить в исключительных случаях, когда в силу объективных обстоятельств допросить лицо в очном режиме не представляется возможным.

В числе безусловно положительных сторон проведения следственных действий в удалённом режиме выделяется возможность обеспечения безопасности его

участников, в особенности тех, которые в такой защите нуждаются ввиду своего процессуального статуса и возраста. Речь идёт прежде всего о несовершеннолетних свидетелях и потерпевших, которые выступают в качестве лиц, уличающих в совершении преступления подозреваемого (обвиняемого) и которые иногда поставлены перед необходимостью отстаивать свою обвинительную позицию на очной ставке с последними. Совершенно очевидно, что принятие решения о проведении этого следственного действия в обычном режиме даётся следователю нелегко, и нередко он отказывается от очной ставки исходя из интересов несовершеннолетнего потерпевшего или свидетеля. Вместе с тем, как отмечают многие, при этом могут быть нарушены права на защиту от обвинения тех участников судопроизводства, в отношении которых они дают показания. Ранее мы уже писали об этом⁶. Ряд учёных и ранее видел выход из этих ситуаций в использовании современных технических средств, позволяющих проводить очную ставку в удалённом режиме, с использованием ВКС, что позволило бы обеспечить для несовершеннолетних участников более комфортные условия, защищающие их от прямого контакта с лицами, которых они могут бояться и в присутствии которых могут отказаться от своих показаний либо подтвердить

⁵ Плахота К. С. Использование следователем (дознавателем) видео-конференц-связи при производстве следственных действий // Известия Тульского государственного университета. Экономические и юридические науки. 2022. № 1. С. 98.

⁶ См. Шишкина Е. В. Проблемы защиты прав несовершеннолетних участников уголовного судопроизводства // Российское право: образование, практика, наука. 2021. № 3. С. 32–39.

показания недобросовестного участника. По мнению П. Г. Смагина, это позволило бы решить обе проблемы: и обеспечить подозреваемым и обвиняемым право на защиту от обвинения, и оградить психику несовершеннолетнего от негативного воздействия⁷.

Полагаем, что нормы ст. 189.1 УПК РФ позволят теперь проводить очные ставки в режиме ВКС с участием несовершеннолетних не только для решения проблем, связанных с удалённостью участников, но и прежде всего с целью обеспечения их безопасности. Определённый интерес вызывают предложения, сформулированные Е. В. Прытковой, которая, исследуя проблемы защиты подозреваемого (обвиняемого), сотрудничающего с правоохранительными органами, предлагает использовать дополнительные средства их защиты и проводить очные ставки посредством видеоконференцсвязи с аудио- и видеопомехами, исключающими идентификацию подозреваемого (обвиняемого), с помощью аналоговых либо цифровых устройств⁸. Полагаем, что искусственно создаваемые помехи могут усложнить и без того непростой процесс восприятия передаваемой допрашиваемыми друг другу информации, что может привести к неверной трактовке услышанного,

введению в заблуждение. Особенно это актуально для несовершеннолетних участников процедуры очной ставки.

В любом случае перед криминалистами сейчас стоят задачи разработки тактических приёмов проведения подобных очных ставок, поскольку обстановка, в которой они будут проводиться, может создавать и иные трудности для несовершеннолетних, связанные и с привыканием к необычным условиям, и с проблемами восприятия на слух передаваемой посредством технических средств информации. Здесь, скорее всего, понадобится довольно продолжительный подготовительный этап установления контакта, привыкания, разъяснения.

Особо сложными в реализации, как нам представляется, будут осуществляемые в режиме ВКС предъявления для опознания. Идентификационная сущность данного следственного действия требует особых условий для восприятия объектов, предъявленных для опознания. В связи с этим существует опасность возникновения помех, затрудняющих визуальное восприятие, и иных факторов, связанных, например, с неблагоприятными условиями в месте нахождения опознаваемого лица, которые усугубляются необходимостью обзора объектов

⁷ Смагин П. Г. Особенности производства очной ставки с участием несовершеннолетних дистанционным способом // Уголовно-процессуальная охрана прав и законных интересов несовершеннолетних. 2019. № 1 (6). С. 131–132.

⁸ Прыткова Е. В. Обеспечение безопасности подозреваемого (обвиняемого), заключившего досудебное соглашение о сотрудничестве, на стадии предварительного расследования уголовно-процессуальные и тактико-криминалистические аспекты: автореф. дис. ... канд. юрид. наук. Санкт-Петербург, 2015. С. 20.

через экран передающего устройства. По мнению Е. В. Прытковой, это следственное действие в подобном режиме необходимо прежде всего для обеспечения безопасности опознающего лица⁹. Однако в законе существует и иной, менее затратный по организационному обеспечению, способ защиты опознающего, закреплённый в ч. 8 ст. 193 УПК РФ. В любом случае, если следователь выберет новый вариант защиты или по иным соображениям будет проводить предъявление для опознания в режиме ВКС, ему предстоит решить вопрос о местонахождении защитника опознаваемого, если он будет принимать участие в этом следственном действии. Защитники нередко заявляют ходатайство с просьбой находиться по месту опознающего лица. Законом этот вопрос не урегулирован, поэтому следователь принимает решение исходя из ситуации. В литературе высказываются различные мнения по этому поводу, в том числе и предложение помещать защитника там, где находится опознающий, чтобы он имел возможность оценивать объективность опознания, предварительно предприняв меры по маскировке внешности опознающего¹⁰. Но в случае применения ВКС, принимая решение, следователь в том числе должен учитывать и то обстоятельство, что защитник может территориально находиться в месте

нахождения своего подзащитного, например, в другом городе.

Даже в традиционном варианте процедура предъявления для опознания сложна и требует чёткой организации и проведения ряда подготовительных мероприятий. В случае проведения предъявления для опознания в режиме ВКС вопросы организации и взаимодействия всех участников приобретают особое тактическое значение, обусловленное его целевой направленностью и специфическими условиями проведения. Полагаем, что предъявление для опознания в режиме ВКС так же, как и допрос, следует проводить в исключительных случаях.

Самостоятельное место в обеспечении процедур проведения следственных действий с применением ВКС занимают вопросы его технического оснащения. Законодатель в ч. 1 ст. 189.1 УПК РФ в качестве условия проведения следственных действий по новым правилам называет наличие у органов расследования технической возможности для таких процедур. Безусловно, реализация этих новелл потребует решения вопросов технической оснащённости органов расследования, что может занять какое-то количество времени. Наличие технических возможностей, в свою очередь, потребует отработки вопросов взаимодействия с

⁹ Прыткова Е. В. Обеспечение безопасности подозреваемого (обвиняемого), заключившего досудебное соглашение о сотрудничестве, на стадии предварительного расследования уголовно-процессуальные и тактико-криминалистические аспекты:

автореф. дис. ... канд. юрид. наук. Санкт-Петербург, 2015. С. 20.

¹⁰ См: Бурыка Д. А. Проблемы организации и тактики предъявления для опознания: [монография]. Москва: Юрлитинформ, 2007. С. 113.

техническим персоналом, обслуживающим это оборудование.

Проблемы, с которыми могут столкнуться следователи и дознаватели при реализации новелл уголовно-процессуального закона в части применения новых технологий, требуют особого тактического сопровождения и разработки целого комплекса рекомендаций. Полагаем, что речь должна идти не об отдельных тактических приёмах, а о комплексном тактико-криминалистическом обеспечении следственных действий,

проводимых в режиме ВКС, которое должно включать в себя вопросы принятия решений о проведении следственного действия в этих условиях, вопросы подготовки и организации взаимодействия с его участниками и лицами, обеспечивающими его проведение, тактические приёмы и комбинации, приспособленные к новым условиям, а также вопросы фиксации полученных результатов и их оформления в соответствии с требованиями закона.

Список литературы

1. Арсенова Н. В. Перспективы применения видеоконференцсвязи в досудебном производстве / Н. В. Арсенова, Е. А. Орлова // Вестник Барнаульского юридического института МВД России. 2020. № 1 (38). С. 136 – 138.
2. Бурыка Д. А. Проблемы организации и тактики предъявления для опознания: [монография]. Москва: Юрлитинформ, 2007. 240 с.
3. Кравец Е. Г. Перспективы использования видеоконференц-связи при производстве следственных действий на досудебных стадиях уголовного судопроизводства / Е. Г. Кравец, Н. В. Шувалов, А. Н. Мартынов // Юридическая наука и правоохранительная практика. 2017. № 4 (42). С. 175–181.
4. Новикова Ю. В. Проблемы и перспективы применения видеоконференц-связи в уголовном процессе // Актуальные проблемы деятельности подразделений УИС: Сборник материалов открытой Всероссийской научно-практической конференции, в 2-х т. (Воронеж, 25 мая 2011 года). Воронеж: Воронежский институт ФСИН России, 2011. С. 375–382.
5. Плахота К. С. Использование следователем (дознавателем) видеоконференц-связи при производстве следственных действий // Известия Тульского государственного университета. Экономические и юридические науки. 2022. № 1. С. 95–102.
6. Прыткова Е. В. Обеспечение безопасности подозреваемого (обвиняемого), заключившего досудебное соглашение о сотрудничестве, на стадии предварительного расследования уголовно-процессуальные и тактико-криминалистические аспекты: автореф. дис. ... канд. юрид. наук. Санкт-Петербург, 2015. 24 с.
7. Смагин П. Г. Особенности производства очной ставки с участием несовершеннолетних дистанционным способом // Уголовно-процессуальная охрана прав и законных интересов несовершеннолетних. 2019. № 1 (6). С. 129– 134.

8. Устинкин П. А. Допрос с использованием систем видео-конференц-связи // Актуальные проблемы борьбы с преступностью: вопросы теории и практики: Материалы XXV международной научно-практической конференции. В 2-х частях (Красноярск, 07–08 августа 2022 года) / отв. ред. Д. В. Ким. Красноярск: Сибирский юридический институт Министерства внутренних дел Российской Федерации, 2022. С. 148–150.

9. Шишкина Е. В. Проблемы защиты прав несовершеннолетних участников уголовного судопроизводства // Российское право: образование, практика, наука. 2021. № 3. С. 32–39.

Elena V. Shishkina

PhD (Law), Associate Professor,
Associate Professor of the Department of Criminalistics,
Ural State Law University named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
evsh18@mail.ru

SOME ASPECTS OF INVESTIGATING ACTION USING VIDEO CONFERENCE

Abstract: The article deals with certain problems that may arise during interrogations, confrontations and presentation for identification using videoconferencing technologies. It is concluded that it is necessary to develop tactical and forensic support for investigative actions conducted using videoconferencing technologies, which should include the issues of making a decision to conduct an investigative action, organizing preparation and interaction with participants, tactics and recommendations for formalizing and fixing its results.

Keywords: investigative actions, video conferencing, tactical and forensic support, interaction.

УДК 343.131.5

Каменев Александр Сергеевич
Адвокат Адвокатской палаты Челябинской области
(г. Челябинск, Российская Федерация)
kamenev_as@rambler.ru

АДВОКАТСКИЙ КОНТРОЛЬ В УГОЛОВНОМ ПРОЦЕССЕ: ЭЛЕКТРОННО-ЦИФРОВОЙ АСПЕКТ

Аннотация: В статье автор обосновывает позицию, согласно которой адвокат наряду с оказанием юридической помощи клиентам по уголовным делам осуществляет контроль за процессуальной, а также организационно-технической деятельностью органов предварительного расследования. Данная функция является эффективным средством защиты прав и законных интересов подзащитных, а также служит дополнительной гарантией обеспечения законности в уголовном процессе при изъятии электронных носителей информации и копирования электронной информации.

Ключевые слова: адвокат, уголовный процесс, электронные носители информации, электронная информация, защита.

Для цитирования:

Каменев А. С. Адвокатский контроль в уголовном процессе: электронно-цифровой аспект // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 129–133.

В последнее время все чаще по уголовным делам принимаются решения на основе имеющихся данных, представленных в электронном виде. Отдельные авторы говорят об электронных доказательствах¹. В связи с этим закономерно возникают вопросы о законности и обоснованности принятых на основании таких

доказательств решений, за которыми следуют процессуальные действия. Принято относить к гарантиям законности прокурорский надзор, судебный и ведомственный контроль. Однако, как показывает практика, сторона защиты, и, прежде всего, защитник — профессиональный адвокат, — также выполняют функцию

¹ См., например: Количенко А. А. Доктринальный подход к определению термина «электронные доказательства» в уголовном процессе // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2021. № 3 (55). С. 136–140; Обидин К. В. Электронное доказательство:

необходимый этап развития уголовного судопроизводства // Актуальные проблемы российского права. 2020. Т. 15, № 11 (120). С. 198–206; Электронные доказательства в уголовном судопроизводстве: учебное пособие для вузов / С. В. Зуев [и др.]; отв. ред. С. В. Зуев. М., 2020.

контроля за деятельностью органов предварительного расследования.

Участие защитника по уголовным делам, как правило, рассматривают под эгидой оказания подзащитному правовой помощи². Это соответствует общей доктрине. Вместе с тем, сторона защиты при ознакомлении с материалами уголовного дела, присутствуя при проведении следственных действий, проводя проверку той или иной информации по собственной инициативе, контролирует деятельность лиц, осуществляющих предварительное расследование. При обнаружении нарушений сторона защиты обжалует действия и решения, обращаясь к прокурору и в суд. Так, по данным Судебного департамента на действия (бездействия) и решения должностных лиц, осуществляющих уголовное производство, в 2020 году по поступившим жалобам в судах находилось на рассмотрении 107472 материала, по которым удовлетворено 4468 обращений³. Нет сомнений в том, что во многом это результат кропотливой работы стороны защиты.

Как отметил Президент РФ В. В. Путин в обращении к участникам и гостям X Всероссийского съезда

адвокатов: «Вы не только защищаете права и законные интересы людей, но и вносите весомый вклад в повышение правовой культуры, укрепление верховенства закона, совершенствование законодательства и правоприменительной практики»⁴.

Опрос следователей органов внутренних дел показал, что большинство из них отрицательно относятся к тому, что грамотный и профессиональный адвокат начинает тщательно проверять материалы уголовного дела. Само участие адвоката в проведении следственного действия накладывает дополнительную ответственность на лицо, производящее расследование.

Вместе с тем, следует согласиться с точкой зрения, согласно которой участие защитника в производстве следственных действий необходимо рассматривать как возможность для следователя исправить допускаемые промахи, обратить внимание на обстоятельства, мимо которых он прошёл или считал не значащими⁵.

Применительно к формированию доказательств в электронном виде контроль со стороны адвоката может осуществляться в

² См.: Закомолдин А. В. Квалифицированная юридическая помощь в уголовном процессе России: понятие, содержание и гарантии: автореф. дис. ... канд. юрид. наук. Самара, 2007; Аксёнов А. Д. Участие защитника в уголовно-процессуальном доказывании: дис. ... канд. юрид. наук. М, 2009.

³ Подобнее об этом см.: Отчет о работе судов общей юрисдикции по рассмотрению уголовных дел по первой инстанции // Судебный департамент при Верховном суде РФ: официальный сайт. URL:

<http://www.cdep.ru/index.php?id=79&item=5671> (дата обращения: 01.05.2022).

⁴ Путин направил приветствие участникам и гостям X Всероссийского съезда адвокатов // ТАСС. 2021. 15 апр. URL: <https://tass.ru/obschestvo/11154891> (дата обращения: 01.05.2022).

⁵ Чебурёнков А. А. Тактическое значение и использование следователем фактора участия защитника в производстве следственных действий // Академическая мысль. 2019. № 3 (8). 126.

таких формах, как: отслеживание порядка изъятия электронных носителей информации и копирование электронной информации при проведении следственных действий; изучение материалов уголовного дела, включая аудио- и видеозаписи, электронные документы на предмет обнаружения ошибок и нарушений закона; обжалование действий и решений по уголовным делам, которые не соответствуют требованиям закона о порядке обращения с электронной информацией; инициирование привлечения к ответственности следователей (дознавателей) за фальсификацию и другие нарушения уголовно-процессуального закона, регламентирующего процесс собирания, проверки и оценки электронных доказательств.

Обратимся к практике.

Так, адвокат в порядке ст. 125 УПК РФ подал в суд жалобу, в которой обратил внимание на незаконные действия оперуполномоченного УЭБиПК, выразившиеся в следующих нарушениях закона: отсутствие постановления о производстве обыска в организации и поручения следователя; непредоставление возможности копировать информацию с изъятых электронных носителей; изъятие не относящихся к расследованию предметов и

документов. Кроме того, адвокат указал, что на изъятых электронных устройствах содержится информация о финансово-хозяйственной деятельности организации, необходимая в повседневной деятельности, изъятые документы на бумажных и электронных носителях являются собственностью организации и необходимы для использования, в том числе в налоговой службе; их отсутствие причиняет убытки. Суд апелляционной инстанции со многими доводами адвоката согласился и направил дело на новое судебное разбирательство.⁶

Другой пример.

В связи с отказом в удовлетворении ходатайства адвоката о копировании информации, содержащейся на электронных носителях, изъятых в ходе обыска, в порядке ст. 125 УПК РФ была подана жалоба в Пресненский районный суд, в ней адвокат просил признать незаконным и необоснованным, по его мнению, постановление следователя по РОВД ГСУ СК России. Суд отказал в удовлетворении жалобы, однако апелляционный суд отменил данное постановление⁷.

Согласно ч. 4 ст. 81 УПК РФ, изъятые в ходе досудебного производства, но не признанные вещественными доказательствами

⁶ Апелляционное постановление Московского городского суда от 05.04.2021 № 10-6648/2021 // Официальный портал судов общей юрисдикции города Москвы. URL: <https://mos-gorsud.ru/mgs/services/cases/appeal-criminal/details/14c620c0-9206-11eb-8a25-73ae24d62004> (дата обращения: 01.05.2022).

⁷ Апелляционное постановление Московского городского суда № 10-186436/2020 // Официальный портал судов общей юрисдикции города Москвы. URL: <https://mos-gorsud.ru/mgs/services/cases/appeal-criminal/details/31ec6eb0-1854-11eb-bb8e-d30cd7dd2439> (дата обращения: 01.05.2022).

предметы, включая электронные носители информации, и документы подлежат возврату лицам, у которых они были изъяты. В противном случае могут быть приняты решения аналогичные *решению Новгородского районного Суда Новгородской области по делу № 2-3844/17, когда с Российской Федерации в лице Следственного комитета Российской Федерации за счёт казны Российской Федерации в пользу К. была взыскана компенсация морального вреда в денежном выражении*⁸.

Особого внимания заслуживают судебные решения об отказе в удовлетворении жалоб защитников на нарушения, допущенные органами предварительного расследования. При этом анализ практики и опрос самих адвокатов показывает, что суды порой «прикрывают глаза на допущенные

нарушения», «латают дыры следствия» и т. п., когда нарушения закона очевидны, — обращения стороны защиты игнорируются или сводятся в ранг незначительных, несущественных. Вместе с тем, страдает законность, а значит, труд адвоката искусственно занижается.

Подводя итог, ещё раз следует отметить, что контроль со стороны адвоката может осуществляться как за процессуальной, так и за организационно-технической деятельностью органов предварительного расследования. Данная функция является эффективным средством защиты прав и законных интересов подзащитных, а также служит дополнительной гарантией обеспечения законности в уголовном судопроизводстве.

Список литературы

1. Аксёнов А. Д. Участие защитника в уголовно-процессуальном доказывании: дис. ... канд. юрид. наук. М, 2009. 213 с.
2. Закомолдин А. В. Квалифицированная юридическая помощь в уголовном процессе России: понятие, содержание и гарантии: автореф. дис. ... канд. юрид. наук. Самара, 2007. 21 с.
3. Количенко А. А. Доктринальный подход к определению термина «электронные доказательства» в уголовном процессе // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2021. № 3 (55). С. 136–140.
4. Обидин К. В. Электронное доказательство: необходимый этап развития уголовного судопроизводства // Актуальные проблемы российского права. 2020. Т. 15, № 11 (120). С. 198–206.
5. Чебурёнков А. А. Тактическое значение и использование следователем фактора участия защитника в производстве следственных действий // Академическая мысль. 2019. № 3 (8). 125–130.

⁸ Решение Новгородского районного суда Новгородской области от 11.10.2017 по делу № 2-3844/2017 // СудАкт. URL:

<https://sudact.ru/regular/doc/TbJrUSZtXu5w/> (дата обращения: 01.05.2022).

6. Электронные доказательства в уголовном судопроизводстве: учебное пособие для вузов / С. В. Зуев [и др.]; отв. ред. С. В. Зуев. М.: Издательство Юрайт, 2020. 193 с.

Alexander S. Kamenev

Attorney at Law of the Chelyabinsk Region
(Chelyabinsk, Russian Federation)
kamenev_as@rambler.ru

**LAWYER'S CONTROL IN CRIMINAL PROCEEDINGS:
ELECTRONIC-DIGITAL ASPECT**

Abstract: In the article, the author substantiates the position according to which the lawyer, along with providing legal assistance to clients in criminal cases, exercises control over the procedural, as well as organizational and technical activities of the preliminary investigation bodies. This function is an effective means of protecting the rights and legitimate interests of the defendants, and also serves as an additional guarantee of legality in criminal proceedings when seizing electronic media and copying electronic information.

Keywords: lawyer, criminal process, electronic media, electronic information, protection.

УДК 004.853

Медведев Виталий Александрович

Преподаватель кафедры социально-экономических и гуманитарных дисциплин,
Ленинградский областной филиал
Санкт-Петербургского университета МВД России
(Ленинградская область, г. Мурино, Российская Федерация)
smit-vint@yandex.ru

ПРОБЛЕМАТИКА ИНТЕГРАЦИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБРАЗОВАТЕЛЬНЫЙ ПРОЦЕСС ПОДГОТОВКИ КАДРОВ ДЛЯ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Аннотация: В статье рассматриваются перспективы внедрения искусственного интеллекта или его элементов в образовательный процесс и возможные проблемы при его внедрении, такие как взаимодействие обучающегося и преподавателя или обучающегося и нейросети. Помимо простых этапов внедрения стоит помнить то, что внедрение искусственного интеллекта не только создаст резонанс в сфере образования, но и в других сферах общественной жизни.

Ключевые слова: искусственный интеллект, образование, нейросеть, преподаватель, обучающийся.

Для цитирования:

Медведев В. А. Проблематика интеграции искусственного интеллекта в образовательный процесс подготовки кадров для органов внутренних дел // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 134–137.

Искусственный интеллект – это будущее. Для того чтобы его обуздать и наладить требуется большое количество времени и средств. Стоит понимать, что на данный момент искусственный интеллект не так развит и распространён, чтобы делать о нём твёрдые выводы. Разные самообучающиеся системы с каждым днём удивляют мировое сообщество всё больше и больше. Показывая, таким образом, что данную технологию нельзя ограничить в вариантах развития.

Искусственный интеллект используется в образовании. В значительной мере он задействуется при подготовке материалов для обучения личного состава. Однако, несмотря на приносимую пользу, искусственный интеллект в этой сфере несовершенен: он не способен понять эмоциональное состояние обучающегося, оказать при необходимости психологическую поддержку. Представляется, что и эти недостатки будут нивелированы со временем, так как искусственный

интеллект разовьёт психологическую эмпатию в процессе своего обучения.

Таким образом, мы видим тенденцию к сохранению формы образования; к сохранению его сущности, цели и пути достижения этой цели разными способами – образование сейчас представлено в широком спектре разнообразных услуг, оказываемых в том числе с участием искусственного интеллекта.

В настоящее время элементы искусственного интеллекта быстрыми темпами внедряются во все сферы деятельности человека. С точки зрения образовательного процесса, несомненно, затраты на создание, воссоздание и приведение к идеалу данного проекта потребуют значительных экономических вложений. Это обуславливается не дороговизной оборудования или сложностью вариаций требуемых кодов, а непосредственным соотношением вложенных в проект средств и временем его развития.

Создание программного кода искусственного интеллекта не займёт много времени. Для реализации самого простого алгоритма искусственного интеллекта и интеграции в этот алгоритм какой-либо простой нейросети, необходимо задействовать не так уж и много ресурсов с точки зрения начального капиталовложения. Однако этап отладки продлится гораздо дольше, нежели этап создания самого макета. Под этапом отладки подразумевается совокупность действий над программным обеспечением и нейросетью, которую трудно как-либо ускорить в нынешнее время. Речь идёт о непосредственном

заполнении базы данных, которая получается благодаря работе с обучающимися и пользователями, а также при получении иной информационной составляющей, которая будет играть большую роль для стабилизации и улучшения работы искусственного интеллекта. Таким образом, введение в действие данной программы потребует больших ресурсных затрат именно в период отладки и при исправлении текущих ошибок, а также при последующем обучении нейросети.

Компенсировать данную проблему будет весьма трудно. Так как искусственный интеллект – сравнительно молодая отрасль техники, – её разработкой могут заниматься лишь высококлассные специалисты в области программирования и учёные, имеющие опыт с настройкой и обучением нейросети, а в нынешних реалиях широкомасштабно данные профессии ещё не распространены, и квалифицированные кадры для такой работы будет подобрать весьма затруднительно. Из этого следует, что работа с нейросетью станет достаточно высокооплачиваемой и перспективной профессией, что в свою очередь не позволит привлекать данных специалистов для работы в органах внутренних дел. Указанный фактор лежит в основе экономического аспекта проблемы повсеместного внедрения систем искусственного интеллекта в образовательные процессы, а также подчёркивает видимое несоответствие затраченных ресурсов и получаемых результатов.

При работе с нейросетями невозможно сейчас однозначно ответить на вопрос о их способности мгновенно найти необходимый подход к тому или иному обучающемуся. На ранних этапах своего создания нейросеть ещё не сможет индивидуально подбирать специальные наборы команд чтобы наверняка гарантировать уяснение обучаемым всей необходимой информации. Данный аспект работы искусственного интеллекта возможно будет реализовать в полной мере лишь при значительном увеличении объёмов хранимых данных об обучении разных людей. Поскольку вариантов решения той или иной задачи у искусственного интеллекта будет много, выбрать нужно будет только один, подходящий для конкретного человека, который будет обучаться по заданной программе.

Также и учитель-человек, лишь становясь опытным преподавателем и набирая необходимый багаж знаний о стереотипах поведения определённых учащихся, их реакциях на ту или иную задачу, сможет моментально понять, как следует объяснить тот или иной материал.

Искусственному интеллекту потребуется две составляющие принятия решения:

- 1) наличие соответствующего материала в базе данных;
- 2) время на поиск этого материала.

Стоит отметить, что уникальных случаев в обучении нет, даже при условии, что программа будет одна и та же. Люди не имеют такого большого количества различных реакций на тот

или иной этап построения задачи, чтобы рано или поздно его не оказалось в готовой базе данных.

Естественно, сразу все необходимые варианты решения задачи не появятся в базе, и нейросеть не сможет наверняка выбрать именно тот вариант решения, который будет приемлем именно для единичного ученика.

Необходимо заметить, что индивидуального подхода обучения можно достичь, но сделать это быстро не получится. Это займёт годы и потребует задействования многих тысяч участников такого типа образования, при условии, что в нейросеть будет загружено несколько алгоритмов действия на тот или иной случай ответа обучающегося, и именно на моменте данного выбора начнётся непосредственное обучение нейросети, а большое число групп тестирования позволит выявить основные способы и методы преподавания обучающемуся определённого материала.

Для того чтобы устранить существенные первичные недостатки искусственного интеллекта в такой серьёзной сфере взаимодействия как образование, необходимо приложить значительные усилия, а также грамотно поэтапно составить план внедрения технологии.

Помимо технических этапов внедрения стоит помнить, что интеграция искусственного интеллекта создаст резонанс не только в той области, на которую непосредственно ориентировано (образовательной в данном случае), но и в других сферах общественной жизни.

Vitaly A. Medvedev

Lecturer of the Department of Socio-economic and Humanitarian Disciplines,
Leningrad Regional branch of
St. Petersburg University of the Ministry of Internal Affairs of Russia
(Leningrad region, Murino, Russian Federation)
smit-vint@yandex.ru

**PROBLEMS OF INTEGRATION OF ARTIFICIAL INTELLIGENCE IN
THE EDUCATIONAL PROCESS OF TRAINING PERSONNEL FOR
INTERNAL AFFAIRS BODIES**

Abstract: The article discusses the prospects for the introduction of artificial intelligence or its elements in the educational process and possible problems in its implementation, such as the interaction of a student and a teacher or a student and a neural network. In addition to the simple implementation steps, it is worth remembering that the introduction of artificial intelligence will not only create a resonance in the field of education, but also in other areas of public life.

Keywords: artificial intelligence, education, neural network, teacher, student.

УДК 341.231

Можаяева Людмила Евгеньевна

Старший преподаватель кафедры теории и истории государства и права,
Гомельский государственный университет имени Франциска Скорины
(г. Гомель, Республика Беларусь)
luda666@yandex.ru

Савченко Дмитрий Геннадьевич

Студент,
Гомельский государственный университет имени Франциска Скорины
(г. Гомель, Республика Беларусь)
savchenko_dmitryi@mail.ru

РЕГУЛИРОВАНИЕ СОЦИАЛЬНЫХ СЕТЕЙ И МЕДИАРЕСУРСОВ КАК ЭЛЕМЕНТ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ

Аннотация: В статье рассматриваются некоторые вопросы обеспечения национальной безопасности Республики Беларусь в условиях постиндустриального общества. Предлагаются правовые новации в области информационного регулирования дезинформации населения, в том числе установления источников такой дезинформации, работы с правосознанием граждан, установления мер юридической ответственности за подобные правонарушения.

Ключевые слова: Республика Беларусь, национальная безопасность, угроза, дезинформация, обеспечение безопасности.

Для цитирования:

Можаяева Л. Е., Савченко Д. Г. Регулирование социальных сетей и медиаресурсов как элемент обеспечения национальной Безопасности Республики Беларусь // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 138–144.

Актуальность рассматриваемой тематики обусловлена имевшими место многократными нарушениями законодательства, как со стороны отдельных лиц, так и групп населения, направленными на насильственный захват и удержание власти методами, противоречащими Конституции Республики Беларусь. Такая

деятельность, являясь экстремистской по направленности, представляет реальную угрозу государственной безопасности как составной части национальной безопасности Республики Беларусь.

Считаем необходимым отметить, что в современном обществе, практически полностью подчинённом

сфере высоких технологий, распространение идеологии экстремизма, её пропаганда, оперативная координация причастных к ней лиц осуществляются с помощью различных мессенджеров, социальных сетей, медиаресурсов.

Подтверждением нашей точки зрения может служить следующая информация: «Главным следственным управлением Следственного комитета Республики Беларусь завершено расследование уголовного дела в отношении администраторов и активных участников деструктивных телеграм-каналов. По данным следствия, в августе прошлого года три женщины и мужчина в возрасте от 28 до 39 лет установили контакт с администраторами и владельцами различных телеграм-каналов и чатов названиями, схожими с «Водители 97%», и начали поиск соучастников для дальнейшей организации групповых действий, грубо нарушающих общественный порядок. В последующем для объединения подобранных соучастников преступления в администрируемых ими открытых и закрытых чатах, группах и телеграм-каналах призывали к блокированию автодорог, повреждению спецтранспорта,

забастовкам и действиям, нарушающим работу общественного транспорта. При этом обвиняемые с целью конспирации регулярно меняли никнеймы и адреса администрируемых ими телеграм-каналов и чатов, рассчитывая, что таким образом им удастся избежать ответственности»¹.

«20 октября 2020 года решением суда Центрального района г. Минска информационный канал интернет мессенджера «Telegram» – «NEXTA-Live» (t.me/nexta_live) и логотип (цифровой водяной знак) «NEXTA» признаны экстремистскими материалами, содержащими информационную продукцию (видеоролики, призывы к публикации как от имени самой редакции канала, так и подписчиков) с признаками экстремистской деятельности, а именно: организация и публичные призывы к осуществлению массовых беспорядков»².

Одновременно с этим, наличествуют факты разоблачения ложной информации, распространяемой в Интернете: «В центре внимания – ложная информация о нарушениях в работе правоохранителей, сообщает БЕЛТА со ссылкой на Telegram-канал пресс-секретаря МВД Ольги Чемодановой»³.

¹ «Блокируем движение в обе стороны»: администраторам телеграм-каналов предъявлено обвинение // Официальный сайт Следственного комитета Республики Беларусь 2021. 17 мар. URL: <https://sk.gov.by/ru/news-ru/view/blokiruem-dvizhenie-v-obe-storony-administratoram-telegram-kanalov-predjjavleno-obvinenie-9786/> (дата обращения: 26.07.2021).

² Верховный Суд Республики Беларусь: официальный сайт. URL:

http://court.gov.by/ru/justice/press_office/685432b980d4453e.html (дата обращения: 26.07.2021).

³ МВД разоблачило фейки о нарушениях в работе правоохранителей // Новости Беларуси|БелТА. 2020. 8 авг. URL: <https://www.belta.by/society/view/mvd-razoblachilo-fejki-o-narushenijah-v-rabote-pravoohranitelej-401997-2020/> (дата обращения: 26.07.2021).

В современном мире люди перестают мыслить сложными категориями, анализировать поступающую информацию, подвергать её разумному сомнению, формировать своё собственное представление о тех или иных событиях, объективно мыслить, основываясь на фактах, историческом опыте. На наш взгляд, причина – колоссальное влияние IT-технологий, значительный объём информации, поступающей, как правило, в готовом виде, не оставляющий времени на осмысление, права на выработку собственной позиции. Такая информация носит характер инструкций, чётко разработанных алгоритмов, призывов к тем или иным деяниям.

Население подвергается массовой дезинформации, которая, как показывает практический опыт, остаётся эффективным инструментом ведения войны, находящимся вне времени:

«Геббельс проводил на восточных землях хитрую политику: он пытался создать у местного населения ощущение спокойной жизни – люди могли смотреть фильмы в кинотеатрах, читать газеты или проводить время на культурных мероприятиях. Народу внушали, что власть большевиков подошла к концу, поэтому им показывали фотографии, на которых солдаты Германии были изображены на фоне московских и ленинградских улиц и

достопримечательностей. Людям говорили, что остатки Красной армии погибают в районе Урала. Все эти фото были смонтированы, и к правде не имели никакого отношения»⁴.

Таким образом, можно наблюдать, что военные технологии, применявшиеся гитлеровской Германией против Советского союза более 70 лет назад, продолжают использоваться заинтересованными лицами в посягательствах на независимость и территориальную целостность Республики Беларусь, с соответствующей адаптацией к современным реалиям, уязвимым местам общественно-политической жизни.

Учитывая, что уровень технического прогресса уже того времени позволял создавать фотоматериалы дезинформационного характера, можно констатировать, что на данный момент создание «фейков» вышло на качественно новый уровень. Современные технологии позволяют добиться ещё более правдоподобного искажения аудиоматериалов, фотографий, видеофайлов, иных форматов представления информации в интересах определённых лиц, так что истинность предложенных материалов не будет вызывать сомнений у целевой аудитории.

Подтверждением могут служить многочисленные факты разоблачения, опровержения такой информации со стороны органов государственной

⁴ Немецкая пропаганда во время Второй мировой войны: главные особенности // Рамблер/новости. 2018. 7 нояб. URL: <https://news.rambler.ru/other/41223090->

[nemetskaya-propaganda-vo-vremya-vtoroy-mirovoy-voyny-glavnye-osobennosti/](https://news.rambler.ru/other/41223090-nemetskaya-propaganda-vo-vremya-vtoroy-mirovoy-voyny-glavnye-osobennosti/) (дата обращения: 27.07.2021).

власти, о которых мы упоминали ранее.

Однако фейки не единственная угроза национальной безопасности Республики Беларусь. По нашему мнению, стоит обратить особое внимание на действия лиц, прямо или косвенно участвующих в незаконных массовых мероприятиях и выступающих якобы за права простого народа, демократию, либеральные идеи и ценности.

Помимо очевидно противоправных акций, они допускают действия обратные избранной идеологии, ущемляющие законные права сограждан: «Во Фрунзенском районе Минска военнослужащие внутренних войск задержали группу людей, у которых изъяты газовые баллончики, электрошокеры, топоры и заточки, а также план-задание на расклейку протестной символики»⁵.

«В течение дежурных суток зарегистрировано два факта ложной занятости железнодорожных путей на перегоне Уша – Олехновичи в Минской области. Задержки движения поездов не было. Следственными органами возбуждено два уголовных дела по данным фактам, а также одно –

в связи с повреждением служебного автотранспорта посредством размещения на автодорогах металлических шипов вблизи деревень Острошицкий Городок и Белые Лужи. Кроме того, неустановленные лица подожгли две автомобильные шины на обочине автодороги при въезде в городской посёлок Руденск Пуховичского района»⁶.

«Всего вчера по стране за нарушение законодательства о массовых мероприятиях и до рассмотрения в суде дел по административным правонарушениям в места содержания задержанных водворён 271 человек. По-прежнему имеют место факты противоправных действий на объектах транспортной инфраструктуры. Так, в Бресте по улице Коммунистической на автодороге неизвестные разбросали гвозди и саморезы, а в Смолевичском районе обнаружен муляж взрывного устройства на железнодорожном полотне, что повлекло вынужденную остановку поезда»⁷.

Помимо этого, нельзя оправдать действия этих лиц идейной борьбой – установлены факты финансирования

⁵ Анонсированные деструктивными Telegram-каналами масштабные протесты не состоялись – МВД // Новости Беларуси|БелТА. 2021. 25 мар. URL: <https://www.belta.by/incident/view/anonsirovanye-destruktivnymi-telegram-kanalami-masshtabnye-protesty-ne-sostojalis-mvd-434415-2021/> (дата обращения: 27.07.2021).

⁶ МВД: за нарушение законодательства о массовых мероприятиях 15 ноября задержаны более 700 человек // Новости Беларуси|БелТА. 2020. 16 нояб. URL: <https://www.belta.by/incident/view/mvd-za->

[narushenie-zakonodatelstva-o-massovyh-meroprijatijah-15-nojabrja-zaderzhany-bolee-700-chelovek-415832-2020/](https://www.belta.by/incident/view/mvd-za-narushenie-zakonodatelstva-o-massovyh-meroprijatijah-15-nojabrja-zaderzhany-bolee-700-chelovek-415832-2020/) (дата обращения: 27.07.2021).

⁷ В Беларуси 13 декабря за нарушение законодательства о массовых мероприятиях задержан 271 человек // Новости Беларуси|БелТА. 2020. 14 дек. URL: <https://www.belta.by/incident/view/v-belarusi-13-dekabrja-za-narushenie-zakonodatelstva-o-massovyh-meroprijatijah-zaderzhan-271-chelovek-420070-2020/> (дата обращения: 27.07.2021).

незаконных массовых мероприятий⁸, которое, что примечательно, осуществляется из-за рубежа. То есть людям платят за то, чтобы они принимали участие в таких мероприятиях⁹.

В такой ситуации, на наш взгляд, нельзя говорить о проявлении высокого уровня правосознания населения, собственного желания народа внести какие-либо изменения в существующий уклад жизни в стране, здесь имеет место лишь обмен суверенитета, богатого исторического прошлого, труда своих предков на деньги, что, помимо прочего, сопровождается отказом анализировать ситуацию, сопоставлять факты, вырабатывать свою позицию. Людям всё преподносится в готовом виде, и они видят то, что хотят видеть, и слышат то, что им слышать выгодно, тем самым, игнорируя выбор большинства¹⁰, пытаются разрушить страну изнутри.

Таким образом перед правоохранительными органами встаёт задача установления того, каким образом значительные массы

населения в короткие сроки смогли обзавестись протестной символикой и атрибутикой, ознакомиться с соответствующими лозунгами и программами, скооперироваться, согласовать вышерассмотренные незаконные действия, а также кому данные действия выгодны. Ведь для этого нужны средства, значительное время для подготовки, особенно, когда данные действия являются заранее разработанными и профинансированными планами захвата власти, так называемыми «цветными революциями», имевшими место во многих постсоветских государствах. На наш взгляд, наиболее яркий и негативный пример – события, начавшиеся в сентябре 2013 года в Украине¹¹, когда отсутствие жёсткой позиции власти, решимости в действиях по отношению к протестующим привели страну в состояние кризиса.

Из вышеприведенного, на наш взгляд, можно сделать следующие выводы, предложить правовые новации:

⁸ СК: установлены неоднократные факты финансирования незаконных массовых мероприятий // Новости Беларуси|БелТА. 2021. 5 фев. URL: <https://www.belta.by/incident/view/sk-ustanovleny-neodnokratnye-fakty-finansirovaniya-nezakonnyh-massovyh-meroprijatij-427231-2021/> (дата обращения: 28.07.2021).

⁹ «Девушкам 60 рублей, парням 30» – Караев рассказал, как финансируются цепочки митингующих в Беларуси // Новости Беларуси|БелТА. 2020. 16 авг. URL: <https://www.belta.by/society/view/devushkam-60-rublej-parnam-30-karaev-rasskazal-kak-finansirujutsja-tsepochki-mitingujuschih-v->

[belarusi-402995-2020/](https://www.belta.by/society/view/devushkam-60-rublej-parnam-30-karaev-rasskazal-kak-finansirujutsja-tsepochki-mitingujuschih-v-belarusi-402995-2020/) (дата обращения: 28.07.2021).

¹⁰ ЦИК утвердил итоги выборов: Президентом избран Лукашенко // Новости Беларуси|БелТА. 2020. 14 авг. URL: <https://www.belta.by/politics/view/tsik-utverdil-itogi-vyborov-prezidentom-izbran-lukashenko-402858-2020/> (дата обращения: 28.07.2021).

¹¹ Украина шесть лет спустя: «евромайдан», который так и не стал «революцией достоинства» // Новости в России и мире – ТАСС. 2020. 21 фев. URL: <https://tass.ru/mezhdunarodnaya-panorama/7798671> (дата обращения: 28.07.2021).

1. На данный момент идёт целенаправленная гибридная война. В этой связи нам необходимо не только не отстать, предпринимая действия оборонительного характера, но и реализовывать решительные контрмеры (контрсанкции, детализация норм, предусматривающих ответственность за вышерассмотренные деяния, усиление идеологической работы с населением).

2. Дополнить статью 188 Уголовного кодекса Республики Беларусь частями 2, 3, 4, 5, 6 следующего содержания:

«2) Распространение заведомо ложной (полностью либо частично) информации либо применение агитации, вводящих другого человека, группу лиц в заблуждение относительно действий органов власти, их должностных лиц, общественно-политической обстановки на территории Республики Беларусь, состояния национальной безопасности, – наказываются лишением свободы на срок от трёх до пяти лет.

3) «Те же действия, совершённые с использованием средств массовой информации, электронной сети Интернет, иных сетей электросвязи общего пользования, медиаресурсов, выделенной сети электросвязи, печатных или публично демонстрируемых произведений, аудио- и видеофайлов, а также во время публичного выступления, – наказываются лишением свободы на срок от шести до десяти лет со штрафом.

4) Действия, предусмотренные частями 2 или 3 настоящей статьи, совершённые в целях совершения преступлений, предусмотренных статьями 356, 357-361², 362-366 настоящего Кодекса, – наказываются лишением свободы на срок от десяти до пятнадцати лет со штрафом.

5) Те же действия, направленные на дестабилизацию промышленности, транспорта, сельского хозяйства, денежной системы, торговли, иных отраслей экономики, деятельности органов государственной власти, организаций, предприятий, иных учреждений с целью ослабления государственной власти или экономики Республики Беларусь, – наказываются лишением свободы на срок от тринадцати до двадцати лет со штрафом.

6) «Действия, предусмотренные частями 2–5 настоящей статьи, повлекшие за собой гибель людей либо сопряжённые с убийством, – наказываются лишением свободы на срок от двадцати до двадцати пяти лет со штрафом, или пожизненным лишением свободы, или смертной казнью».

3. Уже были усилены на законодательном уровне полномочия органов внутренних дел. Так, из общей системы были выделены структурные подразделения и подразделения, осуществляющие борьбу с преступностью в сфере высоких технологий, созданы соответствующие

отдельные управления, с приданием им самостоятельного статуса¹².

4. С целью усиления информированности населения по вопросам информационной безопасности необходимо дополнить учебную программу старших классов по учебному предмету «Обществоведение», а также профессионально-технических, средних специальных и высших учебных заведений, ССУЗов, ВУЗов предметом, название которого, на наш взгляд, может соответствовать

принятому в Республике Беларусь Закону «Борьба с экстремизмом», где учащимся, школьникам и студентам будут разъяснять понятия, содержащиеся в данном нормативном правовом акте, предупреждать их об ответственности за запрещённые деяния экстремистского характера.

Это, на наш взгляд, позволит защитить общество от внешней идейно-ценностной экспансии, деструктивного информационно-психологического воздействия.

Lyudmila E. Mozhayeva

Senior Lecturer of the Department of Theory and History of State and Law,
Francisk Skorina Gomel State University
(Gomel, Republic of Belarus)
luda666@yandex.ru

Dmitryi H. Savchenko

Student,
Francisk Skorina Gomel State University
(Gomel, Republic of Belarus)
savchenko_dmitryi@mail.ru

REGULATION OF SOCIAL NETWORKS AND MEDIA RECOURCES AS AN ELEMENT OF SUPPORTING THE NATIONAL SECURITY OF THE REPUBLIC OF BELARUS

Abstract: The article deals with some issues of national security of the Republic of Belarus in a post-industrial society. It proposes legal innovations in the field of information regulation of disinformation of the population, including the establishment of sources of such disinformation, work with the legal consciousness of citizens, the establishment of legal responsibility for such offenses.

Keywords: The Republic of Belarus, national security, threat, disinformation, security ensuring.

¹² Национальный правовой Интернет-портал Республики Беларусь: официальный сайт. URL:

<https://pravo.by/document/?guid=3871&p0=h10700263> (дата обращения: 29.07.2021).

УДК 336.1.07

Можаева Людмила Евгеньевна

Старший преподаватель кафедры теории и истории государства и права,
Гомельский государственный университет имени Франциска Скорины
(г. Гомель, Республика Беларусь)
luda666@yandex.ru

Савченко Дмитрий Геннадьевич

Студент,
Гомельский государственный университет имени Франциска Скорины
(г. Гомель, Республика Беларусь)
savchenko_dmitryi@mail.ru

ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ В ОРГАНАХ, ОБЕСПЕЧИВАЮЩИХ ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ РЕСПУБЛИКИ БЕЛАРУСЬ

Аннотация: На основании действующего законодательства анализируется опыт Республики Беларусь по внедрению системы электронного документооборота в государственных органах Республики Беларусь, обеспечивающих экономическую безопасность, а также компетенция и степень вовлечённости различных государственных органов в данный процесс.

Ключевые слова: документооборот, IT-технологии, экономическая безопасность, Республика Беларусь, обеспечение безопасности.

Для цитирования:

Можаева Л. Е., Савченко Д. Г. Электронный документооборот в органах, обеспечивающих экономическую безопасность Республики Беларусь // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 145–150.

Тема введения и фактического использования электронного документооборота актуальна в различных государственных органах стран мира. В данном отношении Республика Беларусь, исходя из своего геополитического положения, в целях успешной реализации соответствующего потенциала не может и не должна оставаться в стороне в вопросах, связанных с

применением в различных сферах жизни государства и общества современных IT-технологий, позволяющих вовремя адаптироваться под стремительно изменяющуюся ситуацию на мировой арене, а также быть способной своевременно и адекватно отвечать на новые вызовы и угрозы извне.

Одной из основных проблем любого современного государства

является обеспечение экономической безопасности.

Несмотря на то, что в Республике Беларусь существует специальный орган, а именно Комитет государственного контроля Республики Беларусь (далее – КГК Республики Беларусь), осуществляющий выявление и пресечение правонарушений в экономической сфере, а также наряду с иными, законодательно закреплёнными задачами, осуществляющий защиту интересов государства от противоправных посягательств в экономической сфере, его деятельность, без участия иных органов власти, со смежными целями и задачами, например, Следственного комитета Республики Беларусь (далее – СК Республики Беларусь), органов внутренних дел, органов прокуратуры, государственной безопасности, их структурных подразделений, на данный момент представляется не такой эффективной.

Считаем целесообразным отметить, что документооборот в деятельности вышеупомянутых органов занимает одну из ключевых позиций в процессе реализации ими своих полномочий, так как все действия, предпринимаемые такими органами, в обязательном порядке документируются, в том числе приём и обработка заявлений, обращений граждан и юридических лиц.

Отдельного внимания заслуживают процессуальные документы, без которых невозможно представить ни один процесс, независимо от того, является ли он уголовным, административным либо иным. Также в документах находят

своё выражение локальные акты, в том числе, при межведомственном взаимодействии вышеперечисленных органов в целях повышения эффективности выполнения возложенных на них задач.

В Республике Беларусь законодательство, регулирующее данные отношения, принято не так давно. Остановимся на его характеристике.

К наиболее значимым нормативным правовым актам (далее – НПА) в данной области, на наш взгляд, следует отнести Закон Республики Беларусь от 28.12.2009 г. № 113-3 «Об электронном документе и электронной цифровой подписи», приказ Оперативно-аналитического центра при Президенте Республики Беларусь (далее – ОАЦ) от 08.02.2019 г. № 45 «О дополнительных мерах по реализации Закона Республики Беларусь от 28.12.2009 г. № 113-3 «Об электронном документе и электронной цифровой подписи», приказ ОАЦ от 27.12.2019 г. № 437 «Об утверждении перечня межведомственных информационных систем», приказ ОАЦ от 27.05.2013 г. № 33 «Об утверждении Инструкции о порядке взаимодействия ведомственных систем электронного документооборота государственных органов».

Кратко остановимся на содержании данных нормативных правовых актов.

Основным нормативным правовым актом, регулирующим основы электронного документооборота, является Закон Республики Беларусь от 28.12.2009 г. № 113-3 «Об электронном документе и электронной цифровой подписи».

Данный закон направлен на установление правовых основ применения электронных документов, определение основных требований, предъявляемых к таковым. Также он раскрывает понятие «электронный документ», под которым в соответствии с законом признается «документ в электронном виде с реквизитами, позволяющими установить его целостность и подлинность, которые подтверждаются путём применения сертифицированных средств электронной цифровой подписи с использованием при проверке электронной цифровой подписи открытых ключей организации или физического лица (лиц), подписавших этот электронный документ»¹.

Порядок взаимодействия специально созданных ведомственных систем электронного документооборота с системой межведомственного электронного документооборота государственных органов, предназначенных для обработки служебной информации ограниченного распространения, а также информации, отнесённой к государственным секретам – то есть важнейших сведений, в результате разглашения или утраты которых могут наступить тяжкие последствия, в

том числе для национальной безопасности, – определил приказ ОАЦ от 27.05.2013 №33².

Порядок предоставления организациям и физическим лицам сертификатов открытого ключа электронной цифровой подписи, личного ключа подписи, то есть документов установленной формы, содержащих непосредственно открытый ключ, а также информацию о его владельце, области применения, определяет приказ ОАЦ от 08.02.2019 г. №45. Он также регулирует порядок разработки и утверждения регламента взаимодействия поставщиков услуг в сфере IT-технологий с субъектами информационного взаимодействия Республики Беларусь.

Согласно перечню межведомственных информационных систем, в Республике Беларусь существует пять видов таковых:

- 1) Единая информационная система контроля за выполнением поручений Главы государства;
- 2) Общегосударственная автоматизированная информационная система;
- 3) Система защищённой электронной почты для государственных органов и организаций;

¹ Национальный правовой интернет-портал Республики Беларусь: официальный сайт. URL: [https://pravo.by/document/?guid=2012&oldDoc=2010-15/2010-15\(087-101\).pdf&oldDocPage=1](https://pravo.by/document/?guid=2012&oldDoc=2010-15/2010-15(087-101).pdf&oldDocPage=1) (дата обращения: 06.05.2021).

² Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 27 мая 2013 г. № 33 «Об утверждении Инструкции о порядке взаимодействия

ведомственных систем электронного документооборота с системой межведомственного электронного документооборота государственных органов» // Оперативно-аналитический центр при Президенте Республики Беларусь: официальный сайт. URL: <https://oac.gov.by/public/content/files/files/law/prikaz-oac/2013%20-%2033.pdf> (дата обращения: 07.05.2021).

4) Автоматизированная система государственной защищённой электронной почты ДСП;

5) Система межведомственного электронного документооборота государственных органов Республики Беларусь³.

В Республике Беларусь принимаются меры, направленные на сокращение количества документов на бумажных носителях. Однако внедрение информационно-коммуникативных технологий в деятельность государственных органов на данный момент ещё не завершено, о чём свидетельствует сравнительно небольшое количество нормативных правовых актов в данной области, издающихся с определённой периодичностью.

Отметим, что в КГК Республики Беларусь с 2014 года успешно функционирует система электронного документооборота по следующим направлениям:

- 1) делопроизводство;
- 2) архивное дело;
- 3) гербовые бланки;
- 4) обращения граждан;
- 5) электронная цифровая подпись;
- 6) задания;
- 7) мобильный Канцлер⁴.

По результатам внедрения системы электронного документооборота на платформе

«Канцлер Экспресс» количество бумажных документов в обороте значительно сократилось. Вследствие использования единого механизма работы с документами, значительно повысилась оперативность рассмотрения обращений и принятия соответствующих решений, также ускорился процесс взаимодействия КГК Республики Беларусь с иными государственными органами в рамках деятельности, относящейся к комитету, а также сократились значительные финансовые затраты, присущие бумажному документообороту.

Схожая ситуация наблюдается и в образованном в 2011 году СК Республики Беларусь. В целях оптимизации деятельности руководство СК Республики Беларусь с самых первых дней разрабатывало концептуальные и методологические подходы, технические задания, образовывало специальные группы для создания Единой автоматизированной информационной системы. В целях повышения качества и оперативности работы СК Республики Беларусь в 2018 году было введено программное обеспечение «Е-уголовное дело», систематизирующее уголовные дела, составляющее опись и дающее процессуальные подсказки в целях недопущения совершения ошибки⁵.

³ Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 27 декабря 2019 г. № 437 «Об утверждении перечня межведомственных информационных систем» // Оперативно-аналитический центр при Президенте Республики Беларусь: официальный сайт. URL:

<https://oac.gov.by/public/content/files/files/law/prikaz-oac/2019-437.pdf> (дата обращения: 07.05.2021).

⁴ СЭД «Канцлер» // Официальный сайт. URL: https://kancler.by/print/news/all_news/kgk-19-02-2020.html (дата обращения: 07.05.2021).

⁵ Следственный комитет Беларуси изучил опыт Казахстана по переходу к электронному

Подобные закрытые системы для служебного пользования в целях эффективного выполнения возложенных задач существуют также в органах прокуратуры и внутренних дел с учётом специфики их профессиональной деятельности.

В феврале 2021 года в целях развития информатизации государственного аппарата постановлением Совета Министров Республики Беларусь № 66 была утверждена Государственная программа «Цифровое развитие Беларуси» на 2021–2025 годы. Примечательно, что в данном нормативном правовом акте уделено особое внимание обеспечению стабильности и безопасности работы государственных информационных систем. Так, на период 2021–2025 годов запланировано развитие вышеозначенной Единой автоматизированной информационной системы, однако лишь в части мероприятий по научному обеспечению, развитие информационной системы органов финансовых расследований КГК Республики Беларусь также в части научного обеспечения⁶.

На основании вышеизложенного можно сделать следующие выводы:

1. В Республике Беларусь исключительными полномочиями в сфере государственного регулирования вопросов, связанных с

информационной безопасностью государства, в том числе обеспечением нормального функционирования и защиты информации в процессе электронного документооборота, наделён ОАЦ, в лице специалистов высочайшего класса и уровня профессиональной подготовки.

2. На данный момент в Республике Беларусь существуют различные системы электронного документооборота, однако единой, унифицированной системы, места хранения и перемещения документов нет. На наш взгляд, это связано с ситуацией в мировой экономике, так как разработка и внедрение такой масштабной системы, подготовка соответствующих специалистов потребует значительных финансовых расходов, также велики затраты на обеспечение безопасности, так как взлом или разовый несанкционированный доступ к такой системе, содержащей весь массив документации существующих органов власти, означал бы подрыв национальной безопасности вследствие утечки значительного количества секретной информации.

3. Развитие IT-технологий в сфере документооборота находится в постоянном развитии и совершенствовании, исходя из международных тенденций, опыта других государств, а также состояния национальной экономики.

формату ведения уголовного процесса // Официальный сайт Следственного комитета Республики Беларусь. 2019. 7 авг. URL: <https://sk.gov.by/ru/news-ru/view/sledstvennyj-komitet-belarusi-izuchil-opyt-kazaxstana-poperexodu-k-elektronnomu-formatu-vedenija->

ugolovno-8269/ (дата обращения: 07.05.2021).

⁶ Национальный правовой интернет-портал Республики Беларусь: официальный сайт. URL: <https://pravo.by/document/?guid=12551&p0=C22100066&p1=1> (дата обращения: 08.05.2021).

4. Существование систем внутри- и межведомственного электронного документооборота значительно повысило оперативность взаимодействия для принятия решений органами, обеспечивающими экономическую безопасность государства.

5. Нам представляется, что в обозримом будущем идея Единой автоматизированной информационной системы СК Республики Беларусь будет реализована на практике в полной мере, что также в целом положительно скажется на состоянии экономической безопасности Республики Беларусь за счёт

оптимизации процесса раскрытия преступлений в данной сфере.

Таким образом, большинство решений, предлагавшихся специалистами уже в начале 2000-х, были интеллектуально освоены сферой государственного управления на протяжении последующих 10 лет и так или иначе нашли закрепление в нормативных актах. Это позволяет надеяться, что остающиеся экономические и концептуальные проблемы будут в конце концов преодолены, и перспектива полноценного электронного документооборота реализуется в ближайшее время.

Lyudmila E. Mozhayeva

Senior Lecturer of the Department of Theory and History of State and Law,
Francisk Skorina Gomel State University
(Gomel, Republic of Belarus)
luda666@yandex.ru

Dmitryi H. Savchenko

Student,
Francisk Skorina Gomel State University
(Gomel, Republic of Belarus)
savchenko_dmitryi@mail.ru

ELECTRONIC DOCUMENT CIRCULATION IN AUTHORITIES, PROVIDING ECONOMIC SECURITY OF THE REPUBLIC OF BELARUS

Abstract: Based on the current legislation, the experience of the Republic of Belarus is analyzed in the implementation of an electronic document management system in state bodies of the Republic of Belarus, ensuring economic security, as well as the competence and degree of involvement of various state bodies in this process.

Keywords: document circulation, IT-technologies, economic security, The Republic of Belarus, security providing.

УДК 343.98

Агеева Анастасия Александровна

Преподаватель кафедры конституционного права, адъюнкт,
Уральский юридический институт МВД России
(г. Екатеринбург, Российская Федерация)
zhizhileva74@mail.ru

ПРОБЛЕМЫ ПОЛУЧЕНИЯ И ИСПОЛЬЗОВАНИЯ БИОМЕТРИЧЕСКИХ ДАННЫХ ПРЕСТУПНИКОВ-МИГРАНТОВ

Аннотация: В статье анализируются проблемы, возникающие в сфере использования биометрических данных преступников-мигрантов в процессе расследования преступлений (независимо от этапа расследования). Тенденция информатизации и цифровизации правоохранительной деятельности возрастает, однако, на практике возникают ситуации, осложнённые получением, использованием и непосредственным интерпретированием биометрической информации.

Ключевые слова: биометрические данные, преступник-мигрант, искусственный интеллект, обмен, идентификация, цифровизация.

Для цитирования:

Агеева А. А. Проблемы получения и использования биометрических данных преступников-мигрантов // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 151–156.

Обеспечение национальной безопасности Российской Федерации в современных геополитических условиях является приоритетным направлением деятельности государства. В апреле 2022 года на очередном заседании межведомственной комиссии по совершенствованию государственной миграционной политики Д. А. Медведев (заместитель председателя Совета Безопасности РФ) в очередной раз отметил, что «для нас все так же

важна идея перевода государственных услуг для иностранцев в электронную форму. Делать все процедуры нужно открытыми, понятными, удобными для заявителей. А для государства все эти системы должны стать эффективными, сквозными и полностью прозрачными»¹. Прогрессивное стремительное развитие инновационных технологий находит своё отражение во многих сферах жизни общества, в том числе оно значительно влияет на обеспечение

¹ Кузьмин В. Медведев предлагает запретить въезд мигрантам без биометрии // Российская газета. 2022. 17 апр. № 83 (8731).

URL: <https://rg.ru/2022/04/17/medvedev-predlagaet-zapreshchat-vezd-migrantam-bez-biometrii.html> (дата обращения: 11.05.2022).

правопорядка и защиту государственной безопасности.

В 2021 году были внесены изменения в Федеральный закон от 25 июля 1998 г. № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации», в частности, ст. 9, содержащая в себе перечень субъектов, подлежащих обязательной дактилоскопической регистрации, была дополнена следующими пунктами:

- п) иностранные граждане и лица без гражданства, прибывшие в Российскую Федерацию в целях осуществления трудовой деятельности, в том числе при обращении с заявлением об оформлении патента или при получении разрешения на работу;

- ф) иностранные граждане и лица без гражданства, приобретающие гражданство Российской Федерации;

- х) иностранные граждане и лица без гражданства, прибывшие в Российскую Федерацию в целях, не связанных с осуществлением трудовой деятельности, на срок, превышающий 90 дней со дня въезда в Российскую Федерацию².

Отсюда можно сделать вывод, что сбор персональной и биометрической информации о мигрантах имеет важное стратегическое значение для обеспечения безопасности Российской Федерации.

Следует разобраться в смысловом содержании категории «биометрические данные». В ст. 11 Федерального закона от 27.07.2016 № 152-ФЗ «О персональных данных» под «биометрическими персональными данными» понимаются сведения, которые характеризуют физиологические и биологические особенности человека и на основании которых можно установить его личность³. Биометрические данные представляют собой многоаспектное содержание признаков личности, в том числе преступника-мигранта как элемент криминалистической характеристики преступлений.

Личность преступника-мигранта формируется под влиянием различных факторов (уровень жизни, семейное положение, наличие (отсутствие) законных средств к существованию, поведенческие особенности, причины миграции на территорию другого государства и т. д.). Основная цель приезда иностранных граждан на территорию Российской Федерации – заработок. В ходе проведённого автором работы исследования удалось установить, что большая часть иностранных граждан прибывают на территорию Российской Федерации в весенне-осенний период (сезонная миграция), т. к. основные строительные работы, на которых востребован низкоквалифицированный труд, проводятся в тёплое время года. Таким

² Федеральный закон от 25 июля 1998 г. № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации» // ИПС «Гарант».

URL: <https://base.garant.ru/179140/> (дата обращения: 11.05.2022).

³ Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Российская газета. 2005. 29 июля. № 165.

образом, можно сделать вывод, что востребованность иностранной рабочей силы в РФ остаётся высокой на протяжении 6–9-ти месяцев в году.

Сотрудники полиции (зачастую, это участковые уполномоченные, сотрудники патрульно-постовой службы), проводя поквартирный обход, обход административного участка, выявляют факты совершения противоправной деятельности иностранными гражданами. Поведение иностранных граждан меняется при виде сотрудников полиции (лицо начинает «заливаться краской», меняются манеры поведения, мигрант пытается сделать всё возможное, чтобы не пересечься с сотрудником полиции).

В качестве примеров противоправной деятельности мигрантов могут выступить несколько историй, произошедших в 2021–2022 годах. Так, 27 марта 2022 года недалеко от теплотрассы в одном из районов г. Екатеринбург местная жительница решила покормить собак. В данном месте на неё напал мужчина в чёрной маске – он нанёс ей многочисленные удары по голове бутылкой из-под шампанского, ограбил. Из показаний потерпевшей установлено, что женщина не оказывала сопротивления после нанесения нескольких ударов мужчиной, но он всё равно продолжал избивать её. Врачи констатировали у женщины перелом свода и основания

черепа, в связи с чем, ей потребовалась срочная операция. На сегодняшний день потерпевшая продолжает проходить курсы реабилитации. Обвиняемого задержали: им оказался уроженец (1997 г.) одной из бывших союзных республик, работавший грузчиком в одном из коммерческих предприятий областного центра. Мужчину удалось установить по генетической экспертизе ДНК – на бутылке из-под шампанского осталась его слюна⁴. Свою вину мигрант не признал.

В октябре 2021 года в г. Москва около станции метро «Кузьминки» трое мигрантов избили и ограбили москвича. В ходе исследования записи с камер видеонаблюдения установлено, что прежде, чем скрыться, мигранты ещё и раздели свою жертву, в куртке у потерпевшего, помимо ключей от квартиры, лежали документы, банковская карта и 10 тысяч рублей⁵. Подозреваемых удалось установить по камерам видеонаблюдения, ими оказались граждане ближнего зарубежья 21–24 лет, в момент совершения преступления молодые люди были пьяны. Помимо этого, ранее уже было известно о 26–летнем жителе Обнинска, которого до смерти избили мигранты.

Исходя из анализа приведённых примеров можно сделать вывод, что зачастую иностранные граждане совершают преступления в состоянии

⁴ Казакова Д. Задержан мигрант, напавший на женщину в Екатеринбурге // Информационное агентство «Ura.ru». 2022. 19 апр. URL: <https://ura.news/news/1052546838> (дата обращения: 11.05.2022).

⁵ Кокошкин К. Повалили, избили, раздели, ограбили: мигранты едва не убили москвича у метро // «ЦарьГрад». 2021. 16 окт. URL: https://tsargrad.tv/news/povalili-izbili-razdeli-ograbili-v-migranty-edva-ne-ubili-moskvicha-u-metro_431747 (дата обращения: 11.05.2022).

алкогольного опьянения, не контролируя в должной мере обстановку и отличаясь при этом агрессивностью, импульсивностью. Однако во время допросов мигранты сообщают, что в силу менталитета не употребляют алкоголь в большом количестве. Преступления, совершаемые мигрантами, выявляются в том числе посредством использования биометрической информации – анализ записей с камер видеонаблюдения (на предмет причастности мигрантов к совершённому деянию), изъятия биологических следов в виде слюны (проверка по ДНК), составления фоторобота потерпевшим посредством описания физиологических особенностей преступника-мигранта.

Перспективным представляется использовать здесь технологии искусственного интеллекта, которые способны распознавать отдельные лица на основании их поведенческих и биометрических характеристик, отвечающих требованиям устойчивости, уникальности, универсальности. Биометрия, выступая структурной составляющей криминалистического профилирования, рассматривается в контексте современных криминалистических методов ввиду того, что информационная аналитика (как один из методов криминалистики) на сегодняшний день позволяет обеспечивать правоохранительные органы необходимой информацией. Интерфейсом между теорией и практикой относительно собирания, структурирования, анализа информации выступают информационно-

телекоммуникационные технологии, способные установить, изобличить и идентифицировать определенного субъекта (объекта). При этом всё ещё остаётся нерешённым вопрос, связанный с утечкой персональной информации граждан, использованием её в противоправных целях. Очевидно, что платформа, на которой будет проводиться работа с биометрическими показателями, должна характеризоваться надёжным уровнем защиты и ограниченным правом доступа.

Потребность в обмене информацией, в том числе биометрическими и биографическими данными, касающимися преступной деятельности иностранных граждан очень высока. В связи с этим ведутся работы по созданию централизованной системы, которая будет содержать в себе отпечатки пальцев, фотографии, результаты распознавания лиц и другие соответствующие идентификационные биометрические показатели мигрантов. При этом важно, чтобы сотрудники различных ведомств и подразделений имели доступ к этой базе данных, т. к. только таким образом можно будет повысить уровень раскрываемости преступлений, совершённых мигрантами. В процессе расследования биометрические технологии могут помочь следователю установить наличие (отсутствие) связи какого-либо лица с конкретным деянием, событием, местом, материалом, другим лицом.

Однако необходимо помнить, что полностью исключить негативное влияние человеческого фактора невозможно. Базы оперативных

данных не содержат в себе полной и максимально достоверной информации о личности подозреваемого (обвиняемого), так как при внесении идентификационных сведений каждый сотрудник правоохранительного органа основывается на собственном представлении о значимости того или иного показателя.

Чтобы решить эту проблему, в процессе работы с базами данных биометрических материалов необходимо детально фиксировать объект исследования (предмет преступного посягательства, место преступления и т. д.), а также, с целью недопущения утраты данных, имеющих значение для расследования преступления, обеспечить непрерывную сохранность объекта исследования.

Создание системы биометрических данных (радужная оболочка глаза, изображение лица, ДНК-информация) и отработка правильности их получения в правоохранительной деятельности позволит подтвердить или опровергнуть причастность лица к преступному деянию, детально

прояснить все фактические обстоятельства произошедшего на месте преступления, установить (исключить) наличие причинно-следственной связи подозреваемого с совершённым деянием, событием, местом преступления, идентифицировать неопознанных живых лиц и трупов.

В заключение следует отметить необходимость и колоссальную востребованность использования современных мобильных устройств для сбора данных, так как это позволит сотрудникам полиции осуществлять немедленную проверку «биометрической» информации, полученной от преступника-мигранта. Бесспорно, преступность набирает обороты, существенно опережая научные открытия и достижения, накопленный практический опыт в расследовании, однако использование инновационных подходов в профессиональной деятельности правоохранительных органов, касающихся применения методов современной науки криминалистики способно нивелировать разрыв и повысить эффективность борьбы с преступностью.

Список литературы

1. Кузьмин В. Медведев предлагает запретить въезд мигрантам без биометрии // Российская газета. 2022. 17 апр. № 83 (8731). URL: <https://rg.ru/2022/04/17/medvedev-predlagaet-zapreshchat-vezd-migrantam-bez-biometrii.html>.

Anastasia A. Ageeva

Lecturer in the Department of Constitutional Law, postgraduate student,
Ural Law Institute of the Ministry of Internal Affairs of Russia
(Yekaterinburg, Russian Federation)

PROBLEMS OF OBTAINING AND USE OF BIOMETRIC DATA OF MIGRANT CRIMINALS

Abstract: The article analyzes the problems that arise in the use of biometric data of migrant criminals in the investigation of crimes (regardless of the stage of the investigation). The trend of informatization and digitalization of law enforcement is increasing, but in practice there are situations complicated by the acquisition, use and direct interpretation of biometric information.

Keywords: biometric data, migrant criminal, artificial intelligence, exchange, identification, digitalization.

УДК 343.98

Ржанникова Светлана Сергеевна

Старший преподаватель кафедры криминалистики,
Уральский юридический институт МВД России,
(г. Екатеринбург, Российская Федерация)
ssr80@mail.ru

Лобанов Руслан Эльмирович

Командир отделения 3 курса, курсант,
Уральский юридический институт МВД России,
(г. Екатеринбург, Российская Федерация)
ruslanwww@inbox.ru

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация: В статье рассмотрены правовые и теоретические аспекты применения технологий искусственного интеллекта в правоохранительной деятельности, проанализированы возможности их применения при раскрытии и расследовании преступлений, а также внесены предложения по совершенствованию законодательной регламентации использования данных технологий в деятельности правоохранительных органов.

Ключевые слова: искусственный интеллект, киберпреступность, систематизация информации, программа.

Для цитирования:

Ржанникова С. С., Лобанов Р. Э. Возможности использования искусственного интеллекта в правоохранительной деятельности // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 157–161.

На сегодняшний день информационные технологии шагнули далеко вперёд. Использование искусственного интеллекта в различных областях жизни общества становится всё популярнее. В области правоохранительной деятельности применению искусственного интеллекта уделяется всё больше внимания, поскольку данная технология может помогать

сотрудникам ОВД в раскрытии преступлений, установлении личности преступников и прогнозировании расследования уголовного дела. Актуальной проблемой использования искусственного интеллекта на сегодняшний день остаётся правовая регламентация деятельности лиц, расследующих преступления, а также способности технологий производить определённые действия для создания

условий, способствующих установлению истины по уголовному делу.

В Российской Федерации развитие идеи использования технологий искусственного интеллекта началось с Указа Президента от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации». Законодатель на основании мнения экспертов считает, что благодаря внедрению данных технологий, должно улучшиться качество жизни населения. Следует ожидать аналогичного влияния искусственного интеллекта и на правоохранительную деятельность, поскольку благодаря таким технологиям можно существенно сократить время, затрачиваемое на расследование преступлений.

Существует ещё два нормативно-правовых акта, позволяющих развивать в нашей стране данные технологии. Это Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации», одной из основных целей которого является создание благоприятных условий для разработки и внедрения цифровых инноваций, а также Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных данных"» от 24.04.2020 № 123-ФЗ. В

последнем содержится определение искусственного интеллекта, под которым понимается «комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека». Основная задача экспериментального режима в области правоприменительной практики – это повышение эффективности государственного управления. В свою очередь мы считаем, что необходимо постепенно развивать технологии, применяя их в практической деятельности и законодательно предусмотреть все нюансы, связанные с использованием искусственного интеллекта. Это будет способствовать быстрому внедрению данных технологий в деятельность сотрудников органов внутренних дел.

Несмотря на то, что общество стремится к автоматизации большинства процессов жизнедеятельности, искусственный интеллект не сможет полностью заменить следователя, но способен исключить негативное влияние «человеческого фактора». Также от него следует ожидать значительного вклада в систематизацию деятельности, за счёт предложения различных вариантов расследования.

Одним из основных плюсов развития технологии искусственного интеллекта является предсказание, то есть определение возможных

действий, которые способны повлиять на время и исход расследования преступления, в ближайшем будущем. Так, например, имея статистические данные о преступности в отдельном регионе, можно будет проследить динамику и возможные направления правонарушений, основываясь на анализе собранных материалов.

Следует подчеркнуть, что интеллектуальные системы могут использоваться в качестве навигации в криминалистических базах данных. Однако для этого необходимо предоставить учётную информацию системе на этапе обучения, что вызывает определённые опасения, так как все данные могут быть украдены злоумышленниками в случае нарушения правил информационной безопасности.

Предпосылки развития и внедрения программ с искусственным интеллектом в правоохранительную деятельность есть. Так, в Новом Орлеане (США) с 2012 по 2018 год существовал проект, именуемый как «Палантир», в рамках которого реализовывался процесс сбора информации о человеке: его личности, перемещениях, активности в социальных сетях и пр. Сотрудник полиции мог ввести исходные данные о лице и узнать, что он делал в последнее время. Согласно предоставленным данным, Планер успешно определял лиц с девиантным поведением (80 % преступников, использующих огнестрельное оружие

в качестве реализации преступного умысла). Но у данного проекта существовал большой минус – ни одно преступление не было предотвращено¹.

Как правило, следователю приходится, подчас единолично, заполнять большой объём процессуальных документов, однако развитие технологии и издание НПА, регламентирующих электронный документооборот, позволяют уже сейчас значительно сэкономить временные ресурсы. Системы автозаполнения могут анализировать предоставленные документы, находить связь между исходными данными и помогать следователю в заполнении бумаг. Также не стоит исключать возможность транскрибирования устной речи участника следственных действий, что тоже положительно влияет на скорость работы и принятие решений.

Одним из эффективных направлений использования искусственного интеллекта может стать расследование киберпреступлений. Согласно статистическим данным, предоставленным RTM Group в 2021 году, в России зарегистрировано 518 тыс. киберпреступлений, что на 1,4 % больше, чем в 2020 году². Таким образом, объём работы, стоящей перед сотрудниками правоохранительных органов невероятно велик, и это при том, что киберпреступления достаточно сложны для расследования.

¹ Саблинская И. Предсказать преступление: искусственный интеллект учится разыскивать бандитов // Pravo.ru. 2018. 7 мар. URL: <https://pravo.ru/news/200927/> (дата обращения: 13.05.2022).

² RTM Group: официальный сайт. URL: <https://rtmtech.ru/> (дата обращения: 13.05.2022).

В данной сфере искусственный интеллект позволит анализировать исходные данные операторов и предупреждать правоохранительные органы о готовящемся или совершаемом в сети «Интернет» преступлении. Однако полностью реализовать данную идею возможно, только победив позволяющую оставаться преступникам «в тени» анонимность сети.

Касаемо осмотра электронных носителей информации на предмет обнаружения вредоносного программного обеспечения, использование которого было направлено на завладение, изменение или уничтожение информации, также считаем возможным применение искусственного интеллекта. Зная части исходного кода программы или данные реестра повреждённого компьютера, технология искусственного интеллекта будет способна установить связь между данными злоумышленника и потерпевшего.

Кроме того, технологии искусственного интеллекта постепенно внедряются в такие проекты, как «Умный город» и «Безопасный город». Аппаратно-программный комплекс «Безопасный город» – это совокупность систем, обеспечивающих безопасность населения муниципальных образований. Основная цель данного проекта – обеспечение автоматизированного взаимодействия

различных служб для предупреждения преступности³.

Использование искусственного интеллекта в системе АПК «Безопасный город» вносит немаловажный вклад в раскрытие преступлений. Так, согласно статистическим данным, в 2020 г. было раскрыто 5085 преступлений, из них 2713 краж, 40 убийств, 129 фактов умышленного причинения тяжкого вреда здоровью, 201 разбоев и 516 грабежей⁴.

Данная система способствует профилактике преступности в городах. Установленные камеры видеонаблюдения содействуют предотвращению преступлений в общественных местах, сигнализируя операторам о фактах умышленной порчи имущества, краж и причинения вреда здоровью.

Подводя итог вышесказанному, хотелось бы отметить, что основной проблемой использования искусственного интеллекта в практической деятельности сотрудников органов внутренних дел является его недостаточная правовая и процессуальная регламентация. По своей сути, прогнозирование, систематизация процессов деятельности – это результат эффективной работы программы, возможность использования которой законодательно не закреплена. На наш взгляд, применение данной технологии на постоянной основе в деятельности

³ О «Безопасном городе» // Интернет-портал «Безопасный город». URL: <https://apkgb.info/about/informaciya-o-bg/> (дата обращения: 13.05.2022).

⁴ Свыше 5 тыс. преступлений удалось раскрыть с помощью системы «Безопасный

город» в 2020 году // Официальный сайт ГУ МВД России по г. Москве. URL: <https://77.мвд.рф/news/item/22825421/> (дата обращения: 15.05.2022)

по расследованию преступлений нецелесообразно, потому как любую человеческую деятельность невозможно заменить искусственным интеллектом, её можно только дополнить, открывая новые возможности и способы для расследования преступлений. Однако,

развивать технологии искусственного интеллекта и внедрять их в различные сферы правоохранительной деятельности необходимо, поскольку положительные результаты её использования уже видны по итогам применения АПК «Безопасный город».

Список литературы

1. Саблинская И. Предсказать преступление: искусственный интеллект учится разыскивать бандитов // Pravo.ru. 2018. 7 мар. URL: <https://pravo.ru/news/200927/>.

Svetlana S. Rzhannikova

Senior Lecturer of the Department of Criminalistics,
Ural Law Institute of the Ministry of Internal Affairs of Russia
(Yekaterinburg, Russian Federation)
ssr80@mail.ru

Ruslan E. Lobanov

Cadet,
Ural Law Institute of the Ministry of Internal Affairs of Russia
(Yekaterinburg, Russian Federation)
ruslanwww@inbox.ru

THE POSSIBILITIES OF USING ARTIFICIAL INTELLIGENCE IN LAW ENFORCEMENT

Abstract: The article examines the legal and theoretical aspects of the use of artificial intelligence technologies in law enforcement, analyzes the possibilities of their use in the detection and investigation of crimes, and also makes proposals to improve the legislative regulation of the use of these technologies in law enforcement activities.

Keywords: artificial intelligence, cybercrime, systematization of information, program.

Садыков Мухтар Бейбутович

Докторант,

Академия правоохранительных органов при Генеральной прокуратуре

Республики Казахстан

(г. Косшы, Республика Казахстан)

mukhtar.sadykov@gmail.com

ВНЕДРЕНИЕ АВТОНОМНЫХ СИСТЕМ В ОБЪЕДИНЕННЫХ АРАБСКИХ ЭМИРАТАХ НА ПРИМЕРЕ ПОЛИЦИИ ДУБАЯ: ПРАВОВЫЕ И ТЕХНИЧЕСКИЕ АСПЕКТЫ

Аннотация: В данной статье делается краткий обзор на шаги, предпринятые Объединенными Арабскими Эмиратами (далее – ОАЭ) по развитию автономных систем в стране и её амбициозных целей по занятию лидирующих позиций в этой сфере к 2031 году. В статье термин «автономные системы» охватывает программное обеспечение или алгоритмы робототехники и искусственного интеллекта (ИИ); любая система, которая может функционировать без вмешательства или контроля человека. В статье затронуты вопросы текущего состояния законодательства ОАЭ, регулирующего ответственность автономных систем в рамках гражданского и уголовного законодательства, а также законодательства в области защиты прав потребителей. Также освещены последние разработки в области автономных систем, которые приняты на службу в полицию Дубая, как пример автономных систем в правоохранительной деятельности.

Ключевые слова: искусственный интеллект, автономные системы, Объединенные Арабские Эмираты, правовое регулирование искусственного интеллекта, полиция Дубая, искусственный интеллект в правоохранительной деятельности, ответственность автономных систем.

Для цитирования:

Садыков М. Б. Внедрение автономных систем в Объединенных Арабских Эмиратах на примере полиции Дубая: правовые и технические аспекты // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 162–173.

С начала XXI века Объединенные Арабские Эмираты (далее – ОАЭ) придерживаются дальновидного видения, направленного на построение конкурентоспособной экономики, основанной на знаниях.

В результате сегодня страна занимает 6-е место в мире по внедрению ИКТ, согласно отчету Всемирного экономического форума о глобальной конкурентоспособности за 2019 год. Более конкретно, он занимает первое место в регионе и 19-е место в

мире по Индексу готовности правительства к искусственному интеллекту (далее – ИИ). Кроме того, Дубай занял первое место в мире по привлечению прямых иностранных инвестиций (ПИИ) в области искусственного интеллекта и робототехники, согласно оценкам Ежегодного инвестиционного совещания 2019 года (AIM), инициативы Министерства экономики ОАЭ. В 2015–2018 годах город привлек 21 миллиард долларов США прямых иностранных инвестиций в виде передачи передовых технологий, в то время как Европейский союз (далее – ЕС) и Соединенные Штаты Америки привлекли 5,7 млрд долларов США и 3,9 млрд долларов США соответственно¹.

В 2017 году Объединенные Арабские Эмираты презентовали одну из первых в мире стратегий в области искусственного интеллекта. Цель стратегии – ОАЭ как мировой лидер в сфере искусственного интеллекта к 2031 году. Стоит отметить, что стратегию презентовал первый в мире министр по искусственному интеллекту Омар Султан Аль Олама².

Четкие цели этой стратегии направлены на повышение эффективности и результативности государственного управления на всех

уровнях. Объявлены восемь целей: 1) укрепление позиций ОАЭ как глобального центра искусственного интеллекта; 2) повышение конкурентоспособности сектора искусственного интеллекта в ОАЭ; 3) создание инкубатора для инноваций, связанных с искусственным интеллектом; 4) использование искусственного интеллекта в сфере обслуживания клиентов для улучшения качества жизни; 5) привлечения и обучения талантов для рабочих мест будущего; 6) привлечения ведущих исследовательских возможностей; 7) предоставления инфраструктуры, основанной на данных, для поддержки испытаний ИИ; 8) оптимизации управления и регулирования ИИ. Стратегия охватывает разработку и применение в девяти секторах: транспорт, здравоохранение, космос, образование, возобновляемые источники энергии, окружающая среда, водоснабжение, технологии и дорожное движение³.

В настоящей статье далее будет применяться термин «автономные системы», охватывающий программное обеспечение или алгоритмы робототехники и ИИ, либо любая система, которая может

¹ AlDhaheri S. Building an AI Nation: Accelerating Artificial Intelligence Adoption through Agile Policymaking – the case of the UAE // Dubai Policy Review. 2020. Feb. URL: <https://dubaipolicyreview.ae/building-an-ai-nation-accelerating-artificial-intelligence-adoption-through-agile-policymaking-the-case-of-the-uae/> (accessed: 01.05.2022).

² Brans P. Can UAE become a world leader in AI? // Computer Weekly. 2021. 16 nov. URL:

<https://www.computerweekly.com/news/252509538/Can-UAE-become-a-world-leader-in-AI> (accessed: 24.04.2022).

³ UAE Strategy for Artificial Intelligence // Official portal of the UAE Government. URL: <https://ai.gov.ae/wp-content/uploads/2021/07/UAE-National-Strategy-for-Artificial-Intelligence-2031.pdf> (accessed: 20.04.2022).

функционировать без вмешательства или контроля человека.

Для целей этой статьи термин «автономные системы» охватывает программное обеспечение или алгоритмы робототехники и искусственного интеллекта (ИИ); любая система, которая может функционировать без вмешательства или контроля человека. С юридической точки зрения основное внимание уделяется термину «автономный».

В ОАЭ нет специального закона, регулирующего автономные системы, что означает, что на федеральном или местном уровне не принято закона, который конкретно касался бы регулирования или политики в области искусственного интеллекта.

Однако, существует несколько законов и нормативных актов, которые регулируют ответственность автономных систем, такие как:

- Уголовный кодекс ОАЭ;
- Законы и нормативные акты о защите прав потребителей на федеральном и эмиратском уровнях;
- Правила конфиденциальности данных;
- Закон ОАЭ о гражданских сделках;
- принципы шариата.

В данной статье более подробно рассмотрим ответственность автономных систем в соответствии с Законом ОАЭ о гражданских сделках № 5 от 1985 года («Гражданский кодекс»).

Согласно общему праву, это режим «деликта». В соответствии с Гражданским кодексом ОАЭ (и хотя в некоторых переводах упоминается «деликт») эквивалентным термином

является «действия, причиняющие вред».

Статья 282 Гражданского кодекса ОАЭ гласит, что «любой вред, причиненный другому лицу, делает субъекта, даже если он не является лицом, обладающим правом усмотрения, ответственным за возмещение вреда».

«Вред» делится на две части:

- вред, причиненный лицу;
- ущерб имуществу.

Ответственность требует доказательства ущерба и причинно-следственной связи, что означает, что причиненный ущерб был фактически причинен актом причинения вреда. Если эти условия соблюдены, то лицо, причинившее вред, несет ответственность, а пострадавший имеет право на компенсацию.

Давайте начнем с простого примера: автомобиль сбивает случайного прохожего и травмирует его. Пострадавший имеет право на компенсацию, а водитель несет ответственность, поскольку он не обращал внимания на дорогу.

Теперь рассмотрим тот же пример, но на этот раз тормоза не сработали из-за неисправности: ответственность несет производитель.

Статья 316 Гражданского кодекса ОАЭ гласит, что «Любое лицо, под контролем которого находятся механическое оборудование или вещи, требующие особого ухода, чтобы предотвратить причинение ими ущерба, несет ответственность за любой вред, причиненный такими вещами или оборудованием, за исключением случаев, когда ущерб невозможно было предотвратить».

В обоих приведенных выше примерах мы смогли определить «лицо», будь то физическое или юридическое, стоящее за вредоносным действием.

Такое лицо имеет право на компенсацию. В статье 292 говорится, что «компенсация рассчитывается на основе размера вреда, причиненного жертве, вместе с упущенной выгодой, при условии, что это является естественным результатом вредного деяния».

Таким образом, в режиме ответственности Гражданского кодекса четко обсуждается ответственность «вещей», но разумно предположить, что «вещи» сами по себе не несут ответственности, а лица (будь то юридические или физические лица), стоящие за ними.

А как насчет автономных систем?

Что произойдет, если автономный автомобиль травмирует человека? Кто же тогда несет ответственность? Производитель автомобиля? Проектировщик автономной системы? Дизайнер камер, установленных в автомобиле? Был ли он полностью автономным или полуавтономным (то есть был ли за рулем водитель, который «управлял автомобилем»)? Была ли авария вызвана простой механической неисправностью или более сложной автономной ошибкой в принятии решений, над которой человек не имел никакого контроля?

Статья 291 Гражданского кодекса гласит, что «Если несколько лиц несут ответственность за вредное деяние, каждый из них несет

ответственность пропорционально своей доле в нем, и судья может вынести постановление против них в равных долях или в порядке солидарной или совместной ответственности».

Таким образом, ответственность может быть разделена, если это будет доказано. Но что, если мы не сможем определить, кто несет ответственность? И означает ли это, что в праве есть пробел?

Существующие положения Гражданского кодекса охватывают ответственность за вредные действия и способны защитить пострадавших лиц посредством компенсации. Эти положения, такие как статья 316 об «ответственности вещей», могут быть зеркально отражены для охвата ответственности автономных систем в целом.

Однако в случае полностью автоматизированной системы без контроля со стороны человека существует потенциальный пробел в правилах. По мнению Tarek Nakkach, регионального юридического советника Hewlett-Packard по Ближнему Востоку, этот пробел не обязательно нужно устранять путем изменения существующего режима или внесения поправок в статьи Гражданского кодекса ОАЭ. Составление статьи «охватывающей все случаи» может быть затруднено, ведь для определения первопричин любой неисправности или аварии необходимо больше испытаний автономных транспортных средств.

Для этого требуется огромное количество данных, и у нас пока недостаточно случаев, чтобы создавать

юридические прецеденты и разрабатывать законы или нормативные акты⁴.

Какие средства правовой защиты, доступные лицу, которому был причинен вред автономной системой?

Основными средствами правовой защиты являются гражданские и уголовные. В гражданском иске или иске об ответственности за продукт пострадавшее лицо может потребовать возмещения ущерба. В уголовном иске человек может требовать тюремного заключения, штрафа или дийи (плата за кровь, т. е. возмещение ущерба) в случае смерти.

Гражданский Кодекс

Статья 282 Гражданского Кодекса ОАЭ гласит: «Автор любого правонарушения обязан устранить ущерб».

Бремя доказывания лежит на лице, требующем компенсации; при этом он или она должны показать Суду, представив подтверждающие документы, фактический причиненный ущерб, будь то травма или к примеру, повреждение имущества.

Пострадавшее лицо должно установить, что существует фактический ущерб, а также установить связь между действием системы и полученным ущербом.

Например, в случае автономной медицинской диагностической системы может быть трудно доказать связь между ошибкой в конструкции

системы и причиненным ущербом, в отличие от доказательства связи между человеческой ошибкой, допущенной практикующим врачом в классическом примере медицинской халатности.

В случае контролируемой (не полностью автономной) системы машинного обучения дело может оказаться еще более сложным.

Статья 292 Гражданского кодекса гласит, что «Во всех случаях возмещение определяется в соответствии с суммой вреда, причиненного потерпевшему, вместе с упущенной выгодой, при условии, что это является естественным результатом вредного деяния».

Ущерб или компенсация оцениваются на основе травмы, тяжести и других факторов. В отличие от западных режимов, размер компенсации, присуждаемой судами, обычно невелик.

Суды могут присудить компенсацию не только за физический ущерб, но и за потенциальный моральный ущерб, потерю заработка, потерю возможностей и потенциальный будущий ущерб.

Суды в ОАЭ не обязаны предоставлять основу для расчета компенсации.

Уголовный Кодекс

Если автономная система приводит к травме или смерти, то, в дополнение к праву потерпевшей стороны требовать компенсации в гражданском иске, существует право на уголовный иск.

⁴ Nakkach T. The liability of robotic and autonomous systems – Liability of autonomous systems under the UAE Civil Code // Assuring Autonomy International Programme: website.

URL:
<https://assuringautonomy.medium.com/the-liability-of-robotic-and-autonomous-systems-7ecfa6961409> (accessed: 02.05.2022).

Наиболее вероятно, что вред, причиненный автономной системой, будет квалифицирован как проступок в соответствии со статьей 29 Федерального закона № 3 от 1987 года («Уголовный кодекс»), где средствами правовой защиты являются:

- 1) Задержание;
- 2) Штраф в размере свыше одной тысячи дирхамов;
- 3) Дийа (основанный на законах шариата принцип, эквивалентный компенсации и предоставляемый судами семье умершего лицом, причинившим вред).

Судья может назначить вышеуказанные три санкции одновременно. Однако в статье 299 Гражданского кодекса упоминается, что «Компенсация выплачивается за любой вред, причиненный лицу. При условии, что в случаях, когда выплачивается дийа (плата за кровь) или арш (возмещение ущерба по шариату за телесные повреждения, не приведшие к смерти), они не подлежат выплате в дополнение к такой компенсации, если стороны не договорились об обратном».

Ответственность за продукцию – Закон о защите прав потребителей

Федеральный закон № 24 от 2006 года о защите прав потребителей и его Исполнительный регламент («Закон о защите прав потребителей») – это законодательство, касающееся ответственности за продукцию.

В Законе о защите прав потребителей упоминается, что «поставщики» несут ответственность за дефектные продукты, что означает, что ответственность может нести

любой, кто участвует в обороте продукта, включая производителей и поставщиков.

Нет необходимости доказывать, что поставщик был небрежен, поскольку предполагается обязанность проявлять осторожность, поэтому поставщик будет нести ответственность, если ущерб возникнет из-за дефекта или ошибок в конструкции автономной системы. Это режим, основанный на строгой ответственности, как и западные режимы.

Закон о защите прав потребителей является относительно новым. До сих пор режим защиты прав потребителей использовался в ОАЭ при подаче жалоб на поставщика с требованием ремонта, замены или возврата дефектного продукта.

Пострадавшие лица по-прежнему используют общие положения Гражданского кодекса для требования компенсации за причиненный ущерб, но в случае автономных систем мы можем увидеть рост требований об ответственности за продукцию, используя положения Закона о защите прав потребителей в дополнение к Гражданскому кодексу для получения компенсации.

В заключение рассмотрения правового аспекта функционирования автономных систем следует отметить, что средства правовой защиты – это в основном компенсация, предоставляемая судами. Пострадавшее лицо или лицо, которому был причинен ущерб его или ее имуществу, будет иметь право подать иск против поставщика автономной системы и, возможно,

других лиц, в зависимости от обстоятельств каждого случая и принимая во внимание, что бремя доказывания лежит на заявителе.

Ярким примером использования автономных систем в своей работе является полиция Эмирата Дубай. В структуре полиции есть специальное подразделение по искусственному интеллекту (General Department of Artificial Intelligence)⁵. В апреле 2022 года Исса Ибрагим Басайд, глава отдела приложений искусственного интеллекта и новых технологий в данном подразделении полиции Дубая, был включен в число 30 ведущих арабских экспертов региона в области ИИ по версии MIT Technology Review Arabia⁶.

В 2018 году были запущены первые Умные полицейские участки (Smart Police station), под управлением автономных систем. Умные полицейские участки Дубая открыты 24 часа в сутки, семь дней в неделю и предлагают основные услуги, такие как сообщение о преступлениях, дорожно-транспортных происшествиях и многое другое.

Умные полицейские участки в Дубае используют передовые технологии для сокращения взаимодействия с людьми. Исследования показывают, что некоторые люди чувствуют себя немного напуганными и

обеспокоенными, когда разговаривают напрямую с полицейским. Точно так же другие колеблются из-за отсутствия личной конфиденциальности. Также важно отметить, что языковой барьер является огромным фактором в мультикультурном Дубае.

Умные полицейские участки Дубая устранили эти препятствия, поскольку посетители могут взаимодействовать с системой на семи языках: арабском, английском, французском, испанском, русском, немецком и китайском. Умные полицейские участки предлагают полностью конфиденциальные круглосуточные виртуальные взаимодействия, а посетители имеют прямой доступ ко всем службам.

Они достаточно быстро завоевали доверие жителей Дубая. За первые шесть месяцев 2021 года на этих станциях было обработано более 60 000 транзакций. Кроме того, за тот же период 16 станций посетило 308 865 человек, и они воспользовались интеллектуальными услугами полиции Дубая⁷.

Полиция Дубая не хочет вмешиваться в повседневную жизнь людей, а наблюдает издалека. Программа наблюдения на основе искусственного интеллекта, запущенная в 2018 году, называется Оуооп — по-арабски «глаза». Система может идентифицировать людей или

⁵ Organizational structure // Dubai police official portal. URL: <https://www.dubaipolice.gov.ae/wps/portal/home/aboutus/organizational-hierarchy> (accessed: 01.05.2022).

⁶ Dubai Police officer named among 30 leading Arab artificial intelligence experts // Zawya by Refinitiv. URL:

<https://www.zawya.com/en/legal/dubai-police-officer-named-among-30-leading-arab-artificial-intelligence-experts-e4uq8fyf> (accessed: 04.05.2022).

⁷ All you need to know about Smart Police Stations in Dubai // MyBayut: website. URL: <https://www.bayut.com/mybayut/smart-police-stations-dubai/> (accessed: 04.05.2022).

транспортные средства через обширную сеть камер, а затем передавать информацию в центральную систему. Там их можно сопоставить с существующими базами данных и проанализировать без участия человека. Если поднимается красный флаг, результаты передаются службам экстренного реагирования или другим полицейским управлениям.

Цель полиции Дубая заключалась в том, чтобы заблаговременно выявлять тенденции, выявлять людей, представляющих интерес, и использовать технологии и данные для пресечения преступлений еще до того, как они совершаются, и они называют это «упреждающей» охраной⁸.

Конечно, не все преступления предотвращаются. Но некоторые громкие дела привели к дальнейшему внедрению технологии полицией Дубая.

Одним из них было ограбление в 2007 году в торговом центре Wafi, когда печально известная банда «Розовых пантер» скрылась с драгоценностями на сумму 3,4 миллиона долларов, въехав в торговый центр на автомобилях. После этого дерзкого ограбления власти расширили использование цифровой идентификации.

Точно так же убийство в 2010 году боевика ХАМАСа Махмуда Мабхуха привело к тому, что

количество камер видеонаблюдения в Дубае увеличилось в четыре раза с 25 000 до 100 000.

Используя такое наблюдение и распознавание лиц, Оюн помог арестовать 319 подозреваемых в 2018 году.

В октябре полиция Дубая заявила, что сотрудничает с аналитической фирмой SAS для дальнейшего расширения использования ИИ для «прогнозирования и предотвращения» инцидентов.

Препятствование попаданию наркотиков на улицу является одним из наиболее очевидных примеров предотвращения, и в прошлом году полиция Дубая провела одно из самых крупных арестов, которые город видел за последние годы. С помощью методов искусственного интеллекта «Операция «Сталкер» наблюдала за группой подозреваемых в течение нескольких месяцев до их захвата и изъятия 365 кг героина и кристаллического метамфетамина⁹.

В феврале 2022 года Компания Saudi Technology and Security Comprehensive Control Co. (Tahakom), поддерживаемая Государственным инвестиционным фондом Королевства, подписала соглашение о сотрудничестве с полицией Дубая в области систем искусственного интеллекта, управления дорожным движением и мониторинга нарушений

⁸ How to build an AI-powered (almost invisible) police force // Wired.me: website. URL: <https://wired.me/technology/artificial-intelligence/dubai-police-ai-surveillance/> (accessed: 06.05.2022).

⁹ How to build an AI-powered (almost invisible) police force // Wired.me: website. URL: <https://wired.me/technology/artificial-intelligence/dubai-police-ai-surveillance/> (accessed: 06.05.2022).

для улучшения общественной безопасности.

Ожидается, что сотрудничество между двумя сторонами повысит экономическую ценность, обеспечиваемую оптимальным стилем вождения и передовым подходом к службам дорожного движения, в дополнение к преимуществам искусственного интеллекта для повышения точности обнаружения и предоставления биометрических решений и автоматической идентификации транспортных средств.

Сотрудничество включает в себя предоставление качественных решений для улучшения пересечения дорог и нарушений правил дорожного движения, таких как непристегивание ремней безопасности и использование мобильных телефонов во время вождения, в рамках нескольких основных критериев и показателей, принятых умными городами¹⁰.

Во время ежегодной проверки Главного управления искусственного интеллекта генерал-майор Аль Марри проанализировал некоторые из проектов, в том числе проект, который облегчает пассажирские платежи с помощью интерактивного голосового ответа (IVR), который будет связан с неэкстренным полицейским номером 901.

IVR позволит людям оплачивать свои штрафы и долги в аэропорту, позволяя им беспрепятственно выезжать из страны в случае, если у них есть ожидающие платежи.

Еще одним революционным достижением является использование

дрона Zephyr, высотного псевдоспутника (Haps). Произведенный Airbus, он работает на солнечной энергии и заполняет пробел в возможностях между спутником и БПЛА (беспилотными летательными аппаратами), достигая высоты до 65 000 футов и, таким образом, выходя за рамки гражданской авиации. Его можно использовать для круглосуточной фотосъемки и записи живого видео.

Начальник полиции Дубая также ознакомился с новым изобретением – умным военным костюмом, позволяющим полицейским выполнять свои обязанности в любых обстоятельствах, в дополнение к беспилотному мотоциклу и парящему велосипеду. Он также определил ряд будущих услуг, которые будет предлагать отдел ИИ.

Особого внимания заслуживает новая услуга по переводу денег для заключенных. Заключенные Главного управления исполнения наказаний и исправительных учреждений, подпадающие под определенные категории, теперь могут отправлять и получать деньги посредством перевода, который может осуществляться как внутри страны, так и за ее пределы.

Генерал-майор Аль Марри также ознакомился с новой электронной системой обмена сообщениями и веб-сайтом волонтерских инициатив для сотрудников полиции Дубая, на котором будет проводиться конкурс по управлению волонтерами.

¹⁰ PIF-backed Tahkom, Dubai Police sign deal for AI, traffic management // ArabNews. 2022. 25 feb. URL:

<https://www.arabnews.com/node/2031511/business-economy> (accessed: 07.05.2022).

В Dubai Smart Police Center (SPC) также будет добавлен новый пакет программ, таких как «Парашют» и «Программа свободного рисования», помимо других, помогающих языку жестов, помогающих бороться с торговлей людьми и новой системой информационной безопасности. Новая электрическая линия основного центра обработки данных снизит энергопотребление и обеспечит бесперебойную работу центра.

В рамках инициативы Dubai 10X генерал-майор Аль Марри был проинформирован о программе Smart Interview и чат-ботах, которые будут использоваться для ответов на запросы клиентов на их платформах. Другие инновации включают в себя робота, предназначенного для обслуживания клиентов, интеллектуальную систему патрулирования безопасности, плагин для виртуального смартфона, умные часы на случай чрезвычайных ситуаций и модель 3D-принтера. Также есть клиника искусственного интеллекта и новый электромобиль для оказания технической поддержки, снижения энергопотребления и выбросов углерода, что обеспечивает устойчивость.

Количество сообщений, поступивших в полицию через приложение для iOS и Android, через сервис «Мы все – полиция», за последний год достигло 20 367 сообщений. Сервис запущен для снижения нарушений ПДД и безрассудного вождения в Дубае. Другая служба, «Око полиции», направленная на обеспечение безопасности и снижение уровня преступности, получила в прошлом

году 14 904 сообщения, в том числе 13 904 сообщения через смарт-приложение полиции Дубая и 403 сообщения через веб-сайт.

Все проекты искусственного интеллекта полиции Дубая:

Элегантный военный костюм;

Беспилотный мотоцикл;

Услуга денежных переводов для заключенных;

Чат-боты полиции Дубая;

Робот для обслуживания клиентов;

Умная система патрулирования безопасности;

Плагин виртуального смартфона;

Умные часы на случай чрезвычайных ситуаций;

Модель 3D-принтера;

Клиника искусственного интеллекта.

В заключении, хотелось бы отметить большие успехи ОАЭ, а также полиции Дубая в частности, в сфере внедрения автономных систем и использования их для решения государственных задач. Вместе с тем, в части законодательства, в случае полностью автоматизированной системы без контроля со стороны человека существует потенциальный пробел в правилах. По мнению Tarek Nakkach, регионального юридического советника Hewlett-Packard по Ближнему Востоку, этот пробел не обязательно нужно устранять путем изменения существующего режима или внесения поправок в статьи Гражданского кодекса ОАЭ. Составление статьи «охватывающей все случаи» может быть затруднено, ведь для определения первопричин

любой неисправности или аварии
необходимо больше испытаний
автономных транспортных средств.

Список литературы

1. AlDhaheeri S. Building an AI Nation: Accelerating Artificial Intelligence Adoption through Agile Policymaking – the case of the UAE // Dubai Policy Review. 2020. Feb. URL: <https://dubaipolicyreview.ae/building-an-ai-nation-accelerating-artificial-intelligence-adoption-through-agile-policymaking-the-case-of-the-uae/>.
2. All you need to know about Smart Police Stations in Dubai // MyBayut: website. URL: <https://www.bayut.com/mybayut/smart-police-stations-dubai/>.
3. Brans P. Can UAE become a world leader in AI? // Computer Weekly. 2021. 16 nov. URL: <https://www.computerweekly.com/news/252509538/Can-UAE-become-a-world-leader-in-AI>.
4. Dubai Police officer named among 30 leading Arab artificial intelligence experts // Zawya by Refinitiv. URL: <https://www.zawya.com/en/legal/dubai-police-officer-named-among-30-leading-arab-artificial-intelligence-experts-e4uq8fyt>.
5. How to build an AI-powered (almost invisible) police force // Wired.me: website. URL: <https://wired.me/technology/artificial-intelligence/dubai-police-ai-surveillance/>.
6. Nakkach T. The liability of robotic and autonomous systems – Liability of autonomous systems under the UAE Civil Code // Assuring Autonomy International Programme: website. URL: <https://assuringautonomy.medium.com/the-liability-of-robotic-and-autonomous-systems-7ecfa6961409>.
7. PIF-backed Tahkom, Dubai Police sign deal for AI, traffic management // ArabNews. 2022. 25 feb. URL: <https://www.arabnews.com/node/2031511/business-economy>.
8. UAE Strategy for Artificial Intelligence // Official portal of the UAE Government. URL: <https://ai.gov.ae/wp-content/uploads/2021/07/UAE-National-Strategy-for-Artificial-Intelligence-2031.pdf>.

Mukhtar B. Sadykov

Doctoral candidate,

Academy of Law Enforcement Agencies under the General Prosecutor's Office of the
Republic of Kazakhstan

(Kosshy, Republic of Kazakhstan)

mukhtar.sadykov@gmail.com

INTRODUCTION OF AUTONOMOUS SYSTEMS IN THE UNITED ARAB EMIRATES ON THE EXAMPLE OF THE DUBAI POLICE: LEGAL AND TECHNICAL ASPECTS

Abstract: This article provides a brief overview of the steps taken by the United Arab Emirates (hereinafter referred to as the UAE) to develop autonomous systems in the country and its ambitious goals to take a leading position in this area by 2031. In the article, the term "autonomous systems" covers robotics and artificial intelligence (AI) software or algorithms; any system that can function without human intervention or control. The article touches upon the current state of the UAE legislation governing the responsibility of autonomous systems under civil and criminal law, as well as legislation in the field of consumer protection. It also highlights the latest developments in the field of autonomous systems that have been adopted by the Dubai Police, as an example of autonomous systems in law enforcement.

Keywords: artificial intelligence, autonomous systems, United Arab Emirates, legal regulation of artificial intelligence, Dubai police, artificial intelligence in law enforcement, responsibility of autonomous systems.

Льянов Муса Микаилович

Аспирант кафедры уголовно-правовых дисциплин,
Тюменский государственный университет;
Преподаватель кафедры организации расследования преступлений
и судебных экспертиз,
Тюменский институт повышения квалификации
сотрудников МВД России
(г. Тюмень, Российская Федерация)
musa-lyanov@mail.ru

**ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ОЦИФРОВКИ, ЦИФРОВИЗАЦИИ И
ЦИФРОВОЙ ТРАНСФОРМАЦИИ МАТЕРИАЛЬНЫХ СЛЕДОВ
ПРЕСТУПЛЕНИЯ**

Аннотация: В настоящее время процесс раскрытия и расследования преступлений сложно себе представить без применения современных компьютерных технологий, которые стали его неотъемлемой частью. В связи с этим, одним из главных направлений в работе со следами преступлений становится придание им цифровой формы на электронных носителях информации. Данный процесс в научных исследованиях учёных-криминалистов связывается с такими понятиями как «оцифровка», «цифровизация» и «цифровая трансформация», сущность и особенности которых не имеют чётких границ. Таким образом, в рамках настоящей статьи будут проанализированы имеющиеся подходы к решению данного вопроса, а также предложены оптимальные для целей криминалистики определения.

Ключевые слова: оцифровка, цифровизация, цифровая трансформация, материальные следы, виртуальные следы.

Для цитирования:

Льянов М. М. Теоретические аспекты оцифровки, цифровизации и цифровой трансформации материальных следов преступления // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 180–186.

Современные компьютерные технологии в значительной степени повлияли на процесс фиксации следов, полученных в ходе следственных и иных процессуальных действий. Как показывает практическая деятельность правоохранительных органов,

большинство обнаруженных материальных следов имеют возможность получить своё отражение в цифровом формате.

Стоит отметить, что в настоящее время существует немалое число публикаций, посвящённых переносу

материальных следов в цифровой формат. Таким образом, возникают дискуссии по практическим и теоретическим аспектам процесса такого переноса. В связи с этим, считаем необходимым определить терминологию, которая наилучшим образом могла отразить сущность процедуры придания материальным следам цифрового формата, а также выявить их особенности и дать оптимальные определения рассматриваемым процессам.

Анализ существующих публикаций позволяет сделать вывод о том, что при описании процесса придания цифровой формы объектам материального мира исследователями в основном используются такие термины, как «оцифровка», «цифровизация» и, в некоторых случаях, «цифровая трансформация». При этом каких-либо разграничений в работах учёных-криминалистов между этими понятиями, как правило, не выделяется, что, на наш взгляд, является ошибочным¹.

Так, например, в научной статье А. М. Моисеев под цифровизацией

относительно судебной экспертизы понимает замену аналоговых средств представления объектов их цифровым кодированием².

В работе В. Х. Каримова под цифровой трансформацией (оцифровкой) понимается перевод информации в цифровой код, с которым становится доступен для работы при помощи специализированного программного обеспечения³.

Данные термины встречаются и в других исследованиях, анализ которых, позволяет сделать вывод о том, что «оцифровка», «цифровизация» и «цифровая трансформация»⁴ являются совершенно разными понятиями, которые представляют собой последовательные, всё более глубокие технологические процессы. По нашему мнению, данная позиция является верной и позволяет разграничить особенности исследуемых в настоящей статье процессов от других, схожих по содержанию, но отличающихся по характеру реализации.

¹ Мэнин Х. Типология цифровых организаций в условиях цифровой трансформации // Вестник университета. 2021. № 4. С. 50–56

² Моисеев А. М. Цифровизация коллекций в судебной экспертизе // Вектор науки Тольяттинского государственного университета. Серия: Юридические науки. 2021. № 1 (44). С. 31–38; Иванов Л. Н. Современные проблемы криминалистической биометрии // Информационная безопасность регионов. 2008. № 1 (2). С. 47–55.

³ Каримов В. Х. От чувственно-рациональных методов к цифровой трансформации

криминалистической техники // Сборник материалов криминалистических чтений. 2021. № 18. С. 21–22.

⁴ Шмонин А. В. О некоторых направлениях развития учения о преодолении противодействия расследованию преступлений в условиях цифровой трансформации // Развитие учения о противодействии расследованию преступлений и мерах по его преодолению в условиях цифровой трансформации: Сборник научных статей по материалам международной научно-практической конференции. 2021. С. 312–321.

В связи с вышеизложенным считаем необходимым представить указанные понятия в качестве примера следующим образом:

Под термином «оцифровка» следует понимать процесс придания данным, хранящимся на бумажных и аналоговых носителях, цифрового вида на электронно-цифровых устройствах.

Следующим термином является «цифровизация», который определяется как внедрение в практическую деятельность для повышения её эффективности новых цифровых технологий.

Под термином «цифровая трансформация» следует понимать такое преобразование процессов и явлений, которое предполагает их автоматизацию⁵.

Исходя из вышеизложенного, можно сделать вывод, что наиболее подходящими для рассмотрения вопросов, указанных в настоящей статье, являются термины «оцифровка» и «цифровизация».

Для целей криминалистики термин «оцифровка» можно определить как процесс придания материальным следам преступной деятельности формы двоичного кода, запись которого производится на электронные носители информации при помощи специальных аппаратно-программных технических средств.

Из приведённого определения следуют следующие особенности оцифровки:

1. Она является определенным процессом, который производится по инициативе субъекта оцифровки (следователем, специалистом и т. п.) и направлен на её объекты – материальные следы преступления;

2. Объектом оцифровки являются материальные следы преступления, которые включают в себя предметы, вещества, отображения слеодообразующих объектов, а также обстановку мест совершения преступлений;

3. В результате оцифровки образуется определённый двоичный код на электронном носителе информации, который обусловлен особенностями выбранного для записи носителя, а также фиксируется при помощи специальных аппаратно-программных технических средств.

Деятельность, связанная с непосредственной оцифровкой, записью и хранением полученной информации схожа с процессом работы с виртуальными (электронно-цифровыми, бинарными и т. п.) следами, о чем среди учёных-криминалистов имеется большое количество исследований и публикаций. В связи с этим, в рамках настоящей статьи опустим дискуссию в этой части.

В настоящее время практическая деятельность правоохранительных органов позволяет оцифровать большое количество материальных объектов, которые связаны с расследуемым происшествием. Так, распространение получила оцифровка

⁵ Смушкин А. Б. О семантическом аппарате процесса цифровой трансформации раскрытия расследования и предупреждения преступлений // Криминалистические чтения

на Слобожанщине. Сборник материалов Международной научно-практической конференции. 2021. С. 94–98.

биологических объектов, обнаруженных на месте преступления. Например, в ходе расследования может применяться оцифровка следов папиллярных узоров рук, следов ДНК, создание 3D-моделей мест происшествия и обнаруженных предметов, сканов документов и т. п.⁶

Под цифровизацией в рамках криминалистики, на наш взгляд, следует понимать внедрение в практическую деятельность сотрудников правоохранительных органов новых аппаратно-программных технических средств и баз данных, обеспечивающее повышение эффективности рабочих процессов.

Указанное определение понятия «цифровизация» непосредственно связано с понятием «оцифровка», так как цифровизация обеспечивает процесс оцифровки материальных следов преступлений путём предоставления новых аппаратно-технических средств, а также является её следствием в виде формирования специализированных баз данных.

Из предложенного определения цифровизации можно выделить ряд особенностей:

1. Цифровизация, также как и оцифровка следов преступления, выполняется определёнными субъектами, круг которых, однако, шире. Это объясняется тем, что помимо деятельности по формированию баз данных, которая может выполняться специальными подразделениями правоохранительных органов, она включает также и обеспечение аппаратно-программными техническими средствами, разработка и предоставление которых может выходить за рамки раскрытия и расследования преступлений.

2. Объектами цифровизации являются деятельность правоохранительных органов, а также имеющиеся у них технические и программные средства.

3. Цифровизация деятельности правоохранительных органов может выражаться как в предоставлении аппаратно-программных технических средств, так и в создании специальных баз данных. К числу аппаратно-программных технических средств можно отнести, например, 3D-сканеры, системы по работе с биометрическими данными человека и т. д.⁷ Базы данных, представленные

⁶ Ильиных О. В., Кубрин С. С. Оцифровка 3-х мерных объектов и ее практическое использование // Горный информационно-аналитический бюллетень. 2004. № 6. С. 191–193; Карепанов Н. В. Использование современных технологий при осуществлении криминалистического познания материально фиксированных следов // Наука и технологии XXI века: тренды и перспективы: Сборник статей по итогам IV Профессорского форума. 2021. С. 35–42.

⁷ Маннова А. А., Рожкова В. Р. 3D-сканер: инновации в области криминалистики // Вопросы российской юстиции. 2019. № 3. С. 929–934; Чепрасов М. Г., Колотов М. А. К вопросу о модернизации дактилоскопического учета в современных условиях развития криминалистики на примере построения 3D-дактилоскопической карты // Право и государство: теория и практика. 2017. № 4 (148). С. 147–152; Пилякин М. И. Система бесцветного дактилоскопирования «Папилон». Плюсы и

главным образом учётами, например геномной, дактилоскопической информации и т. п.⁸

4. Внедрённые цифровые технологии повышают эффективность деятельности правоохранительных органов путём предоставления новых возможностей для идентификации лиц, сравнения предметов и документов с имеющимися в базах данных сведениями. Эта особенность цифровизации, в частности, обеспечивается увеличением вычислительных мощностей аппаратно-программных технических средств, ускорения процессов обнаружения, фиксации и изъятия криминалистически значимой информации.

Подводя итог рассмотренным в настоящей статье вопросам, следует отметить, что для понимания процессов, происходящих в практической деятельности правоохранительных органов, необходимо разграничивать понятия «оцифровка», «цифровизация» и «цифровая трансформация». В связи с этим, предлагаем использовать для целей криминалистики предложенные в настоящей статье определения и учитывать выявленные особенности. Также отметим, что сфера оцифровки и цифровизации в криминалистике является дискуссионной и требует дополнительной проработки как теоретических, так и практических аспектов

Список литературы

1. Иванов Л. Н. Современные проблемы криминалистической биометрии // Информационная безопасность регионов. 2008. № 1 (2). С. 47–55.
2. Ильиных О. В. Оцифровка 3-х мерных объектов и ее практическое использование / О. В. Ильиных, С. С. Кубрин // Горный информационно-аналитический бюллетень. 2004. № 6. С. 191–193.
3. Карепанов Н. В. Использование современных технологий при осуществлении криминалистического познания материально фиксированных следов // Наука и технологии XXI века: тренды и перспективы: Сборник статей по итогам IV Профессорского форума. 2021. С. 35–42.
4. Каримов В. Х. От чувственно-рациональных методов к цифровой трансформации криминалистической техники // Сборник материалов криминалистических чтений. 2021. № 18. С. 21–22.
5. Маннова А. А. 3Д-сканер: инновации в области криминалистики / А. А. Маннова, В. Р. Рожкова // Вопросы российской юстиции. 2019. № 3. С. 929–934.

минусы эксплуатации // Вестник Московского университета МВД России. 2013. № 9. С. 126–128.

⁸ Приходько И. С. Совершенствование системы криминалистических учетов в период цифровизации деятельности ОВД //

Вестник Барнаульского юридического института МВД России. 2021. № 2 (41). С. 146–148; Чемерис Д. А., Сагитов А. М., Аминев Ф. Г. Эволюция подходов к ДНК-идентификации личности // Биомика. 2018. Т. 10, № 1. С. 85–140.

6. Моисеев А. М. Цифровизация коллекций в судебной экспертизе // Вектор науки Тольяттинского государственного университета. Серия: Юридические науки. 2021. № 1 (44). С. 31–38.

7. Мэнин Х. Типология цифровых организаций в условиях цифровой трансформации // Вестник университета. 2021. № 4. С. 50–56.

8. Пилякин М. И. Система бескасового дактилоскопирования «Папилон». Плюсы и минусы эксплуатации // Вестник Московского университета МВД России. 2013. № 9. С. 126–128.

9. Приходько И. С. Совершенствование системы криминалистических учетов в период цифровизации деятельности ОВД // Вестник Барнаульского юридического института МВД России. 2021. № 2 (41). С. 146–148.

10. Смушкин А. Б. О семантическом аппарате процесса цифровой трансформации раскрытия расследования и предупреждения преступлений // Криминалистические чтения на слобожанщине: Сборник материалов Международной научно-практической конференции. 2021. С. 94–98.

11. Чепрасов М. Г. К вопросу о модернизации дактилоскопического учета в современных условиях развития криминалистики на примере построения 3D-дактилоскопической карты / М. Г. Чепрасов, М. А. Колотов // Право и государство: теория и практика. 2017. № 4 (148). С. 147–152.

12. Шмонин А. В. О некоторых направлениях развития учения о преодолении противодействия расследованию преступлений в условиях цифровой трансформации // Развитие учения о противодействии расследованию преступлений и мерах по его преодолению в условиях цифровой трансформации: Сборник научных статей по материалам международной научно-практической конференции. 2021. С. 312–321.

13. Эволюция подходов к ДНК-идентификации личности / Д. А. Чемерис, А. М. Сагитов, Ф. Г. Аминев [и др.] // Биомика. 2018. Т. 10, № 1. С. 85–140.

Musa M. Lyanov

Postgraduate student of the Department of Criminal Law Disciplines,
Tyumen State University;

Lecturer at the Department of Organization of Crime Investigation
and Forensic expertise,

Tyumen Institute for Advanced Training
of Employees of the Ministry of Internal Affairs of Russia

(Tyumen, Russian Federation)

musa-lyanov@mail.ru

**THEORETICAL ASPECTS OF DIGITIZATION, DIGITALIZATION AND
DIGITAL TRANSFORMATION
OF MATERIAL TRACES OF A CRIME**

Abstract: At present, the process of detecting and investigating crimes is difficult to imagine without the use of modern computer technologies, which have become its integral part. In this regard, one of the main directions in working with traces of crimes is to give them a digital form on electronic media. This process in the scientific research of forensic scientists is associated with such concepts as «digitization», «digitalization» and «digital transformation», the essence and features of which do not have clear boundaries. Thus, within the framework of this article, the available approaches to solving this issue will be analyzed, as well as optimal definitions for the purposes of forensic science will be proposed.

Keywords: digitization, digitalization, digital transformation, material traces, virtual traces.

УДК 004.738.5

Кириллова Нелли Александровна
Курсант,
Ленинградский областной филиал
Санкт-Петербургского университета МВД России
(Ленинградская область, г. Мурино, Российская Федерация)
nelli.kirillova.03@bk.ru

Медведев Виталий Александрович
Преподаватель кафедры социально-экономических и гуманитарных дисциплин,
Ленинградский областной филиал
Санкт-Петербургского университета МВД России
(Ленинградская область, г. Мурино, Российская Федерация)
smit-vint@yandex.ru

КИБЕРБУЛЛИНГ КАК ОДИН ИЗ ВИДОВ СОЦИАЛЬНОЙ УГРОЗЫ СЕТИ ИНТЕРНЕТ

Аннотация: В статье даётся характеристика Интернет-пространства как социального института, отражаются особенности виртуальной агрессии через социальные сети. Подробно рассматривается кибербуллинг как одна из форм проявления агрессивного поведения в сети Интернет. Рассматриваются возможные методы борьбы с негативными проявлениями кибербуллинга в рамках информационных технологий.

Ключевые слова: Интернет, кибербуллинг, инновационные технологии, коммуникация, киберпространство.

Для цитирования:

Кириллова Н. А., Медведев В. А. Кибербуллинг как один из видов социальной угрозы сети интернет // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 187–192.

Л. С. Высоцкий сказал:
«Ребенок, родившись, уже является социальным существом». В 21 веке эта фраза как никогда актуальна. В наше время высокие информационные связи сделали из человека заложника собственных экспериментов. Общество породило мир технологий и высокого разума и имеет дело с новой,

искусственной природой жизни, при этом не умея предотвращать – ни с повседневной, ни с исследовательской точки зрения – негативные последствия данных инноваций.

Одной из самых распространённых проблем, активно решаемых государственными органами, исследователями и

учёными, является проблема системы «человек-техника». Большое количество технических средств упрощают межличностное взаимодействие, расширяя сферу коммуникативных возможностей человека. Повышается процент передачи информации через всемирную сеть – Интернет, – на базе таких ресурсов, как форумы, телеконференции, электронная почта, IRC (Internet Relay Chat), ICQ.

Стоит отметить, что общение с людьми через посредника – электронные средства – несравнимо с живым общением. В силу вступают новые психологические феномены, которые неизбежно влияют на коммуникацию и изменяют её структуру¹. Виртуальное общение на сегодняшний день вытесняет настоящие эмоции личности, порождает ложное чувство востребованности в обществе, широко распространяясь среди молодого поколения. Основным психологическим явлением, усугубляющим виртуальное общение, является зависимость от электронных средств. На ещё более глубоком психологическом уровне пользователи часто описывают, что их компьютер является продолжением их сознания и личности – «пространство», которое отражает их вкусы, взгляды и интересы. В психоаналитических терминах компьютеры и киберпространство могут стать своего рода «переходным пространством», которое является продолжением внутриспсихического мира индивида.

Оно может переживаться как промежуточная зона между «я» и «другим», которая является частью «я» и частью «другого». Читая на экране электронное письмо, сообщение в группе новостей или чате, написанное товарищем по Интернету, некоторые люди чувствуют, как будто их сознание сливается или смешивается с сознанием другого.

Двое американцев И. Гольдберг и К. Янг, первыми описавшие данное явление, разработали модели интернет-аддикции, представляющей зависимость в виде стремления человека реализовать свои желания, цели, мечты в вымышленной реальности, отчасти от того, что в жизни достичь намеченного не удалось. Ощущение значимости в Интернете приводит к тому, что человек попадает в полную зависимость от электронных средств. В идеальных условиях люди используют это как возможность лучше понять себя, как путь к исследованию своей идентичности, поскольку она связана с идентичностью других людей. В противном случае люди становятся «игрушками» в руках других людей, ими начинают манипулировать. Это может вылиться, например, в кибербуллинг, включающий в себя различные формы оскорблений, прицеливания, унижений личности, шантажа, распространения личных данных и т. д.

Кибербуллинг – это социальная или же электронная травля, обычно определяемая как агрессивное, намеренное действие или поведение,

¹ Рубинштейн С. Л. Основы общей психологии // СПб.: Питер, 2005. 713 с.

которое совершается группой или отдельным человеком неоднократно и в течение долгого периода времени в отношении жертвы, которая не может легко защитить себя².

Российский учёный С. М. Анохин и многие другие исследователи определяют кибербуллинг как намеренные оскорбления, угрозы, распространение порочащих сведений и сообщение другим компрометирующих данных с помощью современных средств коммуникации и в течение продолжительного времени³. Некоторые авторы дополняют понимание анонимностью совершаемых действий. Другие учёные, как русские, так и западные отмечают, что феномен кибербуллинга подразумевает неопределённое количество свидетелей-пособников, которые распространяют негативную информацию и поддерживают её актуальность. Так, Я. Ювонен и Э. Ф. Гросс в своих работах отмечают, что любая атака, связанная с моральным давлением, угнетением и травлей в Интернет-сети, приводящая к отрицательным последствиям, относится к кибербуллингу⁴. Единого мнения о причинах развития, отсутствия эффективных методов борьбы с данным явлением не

сложилось, но в результате постоянной актуализации проблемы интернет-травли удалось достичь определённых результатов.

Так, активное развитие именно данного вида отрицательных электронных взаимоотношений между людьми обуславливается следующими факторами: преступники скрывают свою личность; правонарушители имеют постоянный доступ к объектам нападения; аудитория, которая потенциально подходит для издевательств и травли огромна; преступник не получает быстрой ответной реакции; нет невербальных подсказок о смысле сообщения; изменяется отношение к власти (преступник может иметь мало власти в реальном мире, но обладать высокими технологическими навыками, за счёт чего повышает авторитет в сети); информация, размещаемая в Интернете постоянна⁵.

В последние годы феномен кибербуллинга не только затрагивает ведущие западные страны, но и приносит коррективы в российское информационное пространство. Он заключается в том, что уверенность в сети порождает тенденцию говорить и делать в киберпространстве вещи, которые при личной встрече никогда бы не осуществились. Этот эффект

² Cyber bullying: Its nature and impact in secondary school pupils / P. K. Smith, J. Mahdavi, M. Carvalho [et al.] // Journal of Child and Psychiatry. 2008. Vol. 49. P. 376–385.

³ Анохин С. М., Анохина Н. Ф. Травля учителя – симптом неблагополучия // Народное образование. 2015. № 4. С. 209–212.

⁴ Juvonen J., Gross E. F. Extending the school grounds? // Bullying experiences in cyberspace. Journal of school Health. 2008. Vol. 78 (9).

P. 496–505. Doi: 10.1111/j.1746-1561.2008.00335.x

⁵ Campbell M. Cyber-bullying: An old problem in a new guise? // Australian Journal of Guidance and Counselling. 2005. Vol. 15(1). P. 68–76. Dooley J. J., Pyzalski J., Cross D. Cyberbullying versus face-to-face bullying: A theoretical and conceptual review // Journal of Psychology. 2009. Vol. 217(4). P. 182–188.

способствует увеличению жестокости, продукты которой размещаются или передаются в цифровом формате. Жертвы кибербуллинга подвергаются высокому психологическому давлению со стороны анонимных сообществ, подписчиков, которые распространяют его личные данные (например, контактные данные, адрес проживания, паспортные данные), создают от имени владельца так называемые «фейковые страницы», публикуя ложную информацию, провокационный материал, подрывающие авторитет жертвы. При этом ни государство, ни иные силы не имеют достаточных возможностей, чтобы противодействовать интернет-нарушителям, что вовлекает личность в состояние незащищённости, усугубляя положение.

В роли субъектов кибербуллинга, так называемых преследователей («булли») могут оказаться как близкие, так и совершенно незнакомые люди. Многие участники данного процесса неосознанно выступают пассивными участниками процесса травли – наблюдателями. Не стоит думать, что с интернет травлей сталкиваются только закомплексованные, тихие личности: зачастую этому явлению подвергаются люди, которые вызывают желание у злоумышленников каким-то образом навредить, уничтожить и морально, и психологически.

Соответственно, противодействие системе травли в сети Интернет имеет огромное значение, в силу распространённости феномена кибербуллинга, особенно среди молодого поколения. Россия находится на стадии развития и внедрения

методов борьбы с данной проблемой. Продолжается подбор как теоретических, так и практических методов, исключающих или снижающих процент жертв от кибербуллинга. В подтверждение вышесказанного отметим возможные методы борьбы с негативными проявлениями интернет-взаимодействий:

1) Прямое обучение безопасности в Интернете и надлежащему поведению в киберпространстве. Такое обучение может опираться на стратегии блокирования нарушителей и сообщения о нарушениях. Также широко рекомендуется, чтобы государственная политика по борьбе с издевательствами конкретно ссылалась на кибербуллинг, как на запрещённое поведение.

2) Сохранение персональных данных в рамках информационных технологий.

3) Обращение особого внимания к выкладываемому материалу.

4) Ограничение доступа в социальные сети.

Таким образом, развитие инновационных технологий несомненно двигает прогресс, развитие человечества, но в то же время оно порождает новые проблемы информационного характера. Одним из них стал буллинг, как социальное поведение, сопровождаемое с травлей и агрессивным поведением к жертве. Феноменом 21 века, времени высоких технологий стало понятие кибербуллинг, отождествляющееся с травлей в сети Интернет, которая является серьёзной угрозой мировосприятия и взаимоотношений

людей в обществе. Научные деятели и по сей день выдвигают различные теории о природе зарождения данного поведения в сети, однако данное явление считается малоизученным. Сложность принятия данной проблемы состоит в несформированном понятийном аппарате кибербуллинга в законодательстве, включающем в себя, отсутствие определения основного понятия и способов борьбы с ним. При этом совершенно очевидно, что борьба с ним реальна, однако требует задействования сил широких слоёв населения, образования людей в этой сфере, срочной разработки охранительных мер, влекущих негативные последствия для нарушителей. Важно комплексно охватить данную тему, прибегая к обучению родителей и педагогов, а также к психологической подготовке детей и подростков. Но главным и

решающим фактором является повышение индивидуальной сознательности, культурного воспитания и уважения к окружающим людям, что представляет наибольшую трудность в век «зомбированности» в электронной сети и отсутствия проявления «живых», настоящих эмоций. Решая данную проблему, стоит прислушаться к ведущим исследователям и не демонстрировать толерантное поведение в проявлении травли и унижений. Россия есть и будет страной великих ценностей, норм и принципов, которая готова отстаивать интересы ближнего. Благодаря великому историческому прошлому, традициям, которые почитаемы в народах нашей необъятной Родины, можно говорить о стремлении и возможности победить негативные стороны цифрового общества.

Список литературы

1. Анохин С. М. Травля учителя – симптом неблагополучия / С. М. Анохин, Н. Ф. Анохина // Народное образование. 2015. № 4. С. 209–212.
2. Баранов А. А. Кибербуллинг – новая форма угрозы безопасности личности подростка / А. А. Баранов, С. В. Рожина // Вестник Балтийского федерального университета им. И. Канта. 2015. № 11. С. 61–66.
3. Ефимова Т. В. Интернет и подростковая агрессивность: грани проблемы / Т. В. Ефимова, А. Г. Береснева // СИСП. 2016. № 8 (64). С. 108–116.
4. Кобец П. Н. Противодействие угрозам киберсталкинга – важнейшей проблеме, исследуемой в рамках совершенствования аспектов информационной безопасности регионов в условиях глобализации информационного пространства // Вестник Прикамского социального института. 2017. № 1 (76). С. 27–35.
5. Рубинштейн С. Л. Основы общей психологии // СПб.: Питер, 2005. 713 с.
6. Campbell M. Cyber-bullying: An old problem in a new guise? // Australian Journal of Guidance and Counselling. 2005. Vol. 15(1). P. 68–76.
7. Cyber bullying: Its nature and impact in secondary school pupils / P. K. Smith, J. Mahdavi, M. Carvalho [et al.] // Journal of Child and Psychiatry. 2008. Vol. 49. P. 376–385.

8. Dooley J. J. Cyberbullying versus face-to-face bullying: A theoretical and conceptual review / J. J. Dooley, J. Pyzalski, D. Cross // Journal of Psychology. 2009. Vol. 217(4). P. 182–188.

9. Juvonen J. Extending the school grounds? / J. Juvonen, E. F. Gross // Bullying experiences in cyberspace. Journal of school Health. 2008. Vol. 78 (9). P. 496–505. Doi: 10.1111/j.1746-1561.2008.00335.x

Nelli A. Kirillova

Cadet,

Leningrad regional branch of

St. Petersburg University of the Ministry of Internal Affairs of Russia

(Leningrad region, Murino, Russian Federation)

nelly.kirillova.03@bk.ru

Vitaly A. Medvedev

Lecturer of the Department of Socio-economic and Humanitarian Disciplines,

Leningrad Regional branch of

St. Petersburg University of the Ministry of Internal Affairs of Russia

(Leningrad region, Murino, Russian Federation)

smit-vint@yandex.ru

CYBERBULLYING AS ONE OF THE TYPES OF SOCIAL THREATS ON THE INTERNET

Abstract: The article characterizes the Internet - space as a social institution, reflects the features of virtual aggression through social networks. Cyberbullying is considered in detail as one of the forms of manifestation of aggressive behavior on the Internet. Possible methods of combating the negative manifestations of cyberbullying in the framework of information technology are considered.

Keywords: Internet, cyberbullying, innovative technologies, communication, cyberspace.

УДК 343.72

Рожков Роман Александрович

Курсант,

Ленинградский областной филиал

Санкт-Петербургского университета МВД России

(Ленинградская область, г. Мурино, Российская Федерация)

rojkov.roman2018@yandex.ru

Медведев Виталий Александрович

Преподаватель кафедры социально-экономических и гуманитарных дисциплин,

Ленинградский областной филиал

Санкт-Петербургского университета МВД России

(Ленинградская область, г. Мурино, Российская Федерация)

smit-vint@yandex.ru

К ВОПРОСУ О СПОСОБАХ ИНТЕРНЕТ-МОШЕННИЧЕСТВА

Аннотация: В статье рассматриваются способы интернет-мошенничества, которые в настоящее время активно применяются злоумышленниками с целью получения необходимой информации за счёт человеческих слабостей. То есть через средства социальной инженерии, направленные на то, чтобы обманом заставить человека раскрыть информацию о себе или предоставить доступ к различным данным.

Ключевые слова: кибербезопасность, скам, фишинг, персональные данные, мошенничество.

Для цитирования:

Рожков Р. А., Медведев В. А. К вопросу о способах интернет-мошенничества // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 193–196.

Информация – один из важнейших активов человека, компании, объединения. Она может составлять коммерческую тайну, т. е. при существующих или возможных обстоятельствах способствовать увеличению доходов, избеганию неоправданных расходов, или получению иной коммерческой выгоды. Говоря об обеспечении кибербезопасности, большинство

думает о том, как защититься от хакеров, использующих технические уязвимости сетей. Но есть и другой способ получения необходимой информации мошенниками – через человеческие слабости. Такой путь называется социальной инженерией – он позволяет обманом заставить кого-то раскрыть информацию или предоставить доступ к различным данным. Мошенники манипулируют

людьми, чтобы получить от них информацию или доступ к ней. В настоящее время распространён такой тип афер, как «СКАМ» – один из видов интернет-мошенничества, при котором мошенники намереваются получить какую-либо выгоду путём установления личных отношений через интернет. В отличие от спама (несанкционированной рассылки рекламы) или фишинга, когда жертву обманывают посредством технических приёмов, скам строится на индивидуальной «психообработке» жертвы. СКАМ – процесс получения денежных средств преступным путём, посредством самостоятельного перевода средств жертвой на нужный счёт. Например, некто, притворяясь сотрудником службы поддержки, может попросить пользователей сообщить их пароли. Удивительно, но люди довольно часто добровольно выдают эти данные, особенно если им кажется, что запрос поступает от уполномоченного лица (телефонный скам).

В зависимости от подготовки жертвы для хищения средств выделяется несколько схем такого типа мошенничества, самые популярные из них:

«Мамонт» – самая распространённая схема мошенничества, заключающаяся в создании злоумышленником объявления о продаже определённого товара на интернет-сервисе и оформлении доставки через поддельный сайт. Пик мошеннической активности данного вида пришёлся на 2020 год в связи с пандемией, ведущей за собой увеличение спроса на онлайн-покупки и услуги курьерской доставки.

Если «мамонт» является первой в списке самых распространённых схем скама, то «белый кролик» по праву занимает второе место в этом рейтинге. Эта схема базируется на подделке популярных сайтов по продаже вещей или услуг. Когда предполагаемая жертва попадает на поддельный сайт, её внимание сразу обращается на какой-либо конкурс, розыгрыш или скидки невиданной щедрости. Сразу разоблачить скам-ресурс не получится: сайт выглядит так же, как официальный, различие заключается только в домене.

Чуть сложнее организована работа крупных скам-проектов. Каждый современный человек, использующий социальные сети не только для коммуникации, но и для сёрфинга, чтения новостей, однажды встречал рекламные объявления с предложением лёгкого заработка или удачного вложения денег с поражающей окупаемостью. Деятельность выкладывающих данные объявления организаций построена на людской наивности и азартности. Основные признаки таких проектов: прибыль за счёт привлечения новых вкладчиков и ограниченный доступ к учредительным документам, финансовой отчётности компании.

В связи с пандемией большинство школ, университетов перешло на дистанционное обучение и многие студенты, старшеклассники, проводящие огромное количество времени за компьютером, старались найти способы для заработка из дома. Как показывает практика, в поисках лёгкого заработка многие либо попадались на уловки мошенников,

либо сами решались заработать не совсем легальным способом.

В грёзах о богатстве люди часто идут на неоправданные риски, иногда настолько серьезные, что вмиг лишаются перспектив на успешную карьеру. Дела, связанные с мошенничеством, рассматривает отдел по борьбе с экономическими преступлениями.

Скам квалифицируется в УК РФ по статье 159.6 «Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путём ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей».

Суммарно на компьютерное мошенничество приходится 73 % всех киберпреступлений в интернете, из них 56 % – на скам (обман с добровольным платежом и раскрытием своих данных) и 17 % – на фишинг (кража данных банковских карт). Благодаря лишь одной популярной схеме, получившей название «Мамонт», 70 активных мошеннических групп, 54 из которых нацелены на Россию, менее чем за год похитили у пользователей около 700 млн руб.

Несмотря на то, что мошеннические схемы постоянно прогрессируют, развиваются и усложняются, ежедневно раскрывается огромное количество преступлений, совершённых на этой почве.

Трудности, с которыми сталкиваются сотрудники полиции в противодействии преступлениям такого типа, это: использование мошенниками VPN и сетей Wi-Fi общего пользования, например в торговых центрах и кофейнях.

Действительно, проблема мошенничества в сети сейчас как никогда актуальна, никто из нас не может быть абсолютно защищён от действий злоумышленников. В такое непростое время, как пандемия, мы стали больше зависеть от интернета: появилась удалённая работа, активно используется доставка продуктов, и в некоторых школах из-за ограничений даже проводился онлайн выпускной. Это буквально «райское» время для мошенников. К счастью, как во многих учебных заведениях, так и на просторах интернета, начали проводиться занятия по обеспечению собственной безопасности в интернете, на которых освещаются основные способы защиты от утечки личных данных и средств. Чтобы обезопасить себя, близких и не оказаться жертвой мошенников, Роспотребнадзор рекомендует придерживаться нескольких правил. Самое важное из них – бережно относиться к своим персональным данным и документам. Это касается как данных карты, так и данных вашего паспорта, адреса и т. д.

В заключение можно отметить, что лучшая защита от мошенников – это ответственное обращение человека со своими личными данными.

Roman A. Rozhkov

Cadet,

Leningrad regional branch of

St. Petersburg University of the Ministry of Internal Affairs of Russia

(Leningrad region, Murino, Russian Federation)

aveter254@gmail.com

Vitaly A. Medvedev

Lecturer of the Department of Socio-economic and Humanitarian Disciplines,

Leningrad Regional branch of

St. Petersburg University of the Ministry of Internal Affairs of Russia

(Leningrad region, Murino, Russian Federation)

smit-vint@yandex.ru

TO THE QUESTION ABOUT WAYS OF THE INTERNET – FRAUD

Abstract: The article discusses the method of Internet fraud, which are currently actively used by attackers in order to obtain the necessary information through human weaknesses. That is, through the means of social engineering, namely, by tricking a person into revealing information about himself or providing access to various data.

Keywords: cybersecurity, scam, phishing, personal data, fraud.

УДК 340

Коваленко Наталья Евгеньевна
Магистрант,
Алтайский государственный университет
(г. Барнаул, Российская Федерация)
Kovalenkorub5@gmail.com

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ПРАВО НА УЧАСТИЕ В ПРАВООТНОШЕНИИ В КАЧЕСТВЕ СУБЪЕКТА

Аннотация: В статье рассматривает вопрос отнесения искусственного интеллекта и его юнитов к категории субъектов права, в том числе субъектов правоотношения. Приведена теория Л. И. Петражицкого для сравнительного анализа положения ИИ и ЮЛ, так как они выступают не классическими категориями с точки зрения субъекта права в лице человека. Сделан вывод об истинности субъекта права, которым является непосредственно человек.

Ключевые слова: искусственный интеллект, субъект права, субъект правоотношений, правоотношение, теория права, антропоцентричность права.

Для цитирования:

Коваленко Н. Е. Искусственный интеллект: право на участие в правоотношениях в качестве субъекта // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 197–199.

В настоящее время активно ведутся дискуссии об определении места искусственного интеллекта и его юнитов в структуре правоотношения, точнее встаёт вопрос о признании его субъектом правоотношения. При этом характеристики свойственные субъекту не подвергаются детальному анализу, что является несомненным упущением, в результате чего ИИ ошибочно имеют субъектом права.

Субъект права – человек, обладающий свойственным ему индивидуальным правосознанием, набором морально-ценностных ориентиров, волевой детерминантой. Ни один продукт цифровизации, в том

числе искусственный интеллект, не способен на сопереживание, моральную оценку социальных отношений, в том числе правоотношений, к примеру, что ярко демонстрирует институт судейского усмотрения.

Таким образом, происходит подмена понятий при наделении ИИ и его юнитов в соответствующих отношениях статусом субъекта права. В данном случае целесообразно привести тезис профессора А. В. Габова, который описал возникшую ситуацию: как субъектно-объектную реальность. Из классического подхода к субъекту права вынимают сущность,

в большей степени неотделимую от человека и оставляют структурное содержание «субъекта права», тем самым происходит «поглощение субъекта структурой»¹.

Обратимся к работе «Теория права и государства в связи с теорией нравственности» Л. И. Петражицкого. Так, рассматривая концепцию правоотношения, он детально исследовал вопрос субъектов: учёный проанализировал позиции современников: теории фикции, целевых имуществ, бессубъектных прав и т. д. Л. И. Петражицкий подверг их критике, хотя тот факт, что их объединяет приверженность к характеристике субъекта права через личность или образ человека, явно могло положительно оцениваться учёным-правоведом². «Юридические лица играют в науке права такую же роль, как чучела для пугания воробьёв в антропологии, если бы их отнести туда как особый вид людей, потому что они изображают человека»³. Соответственно, если рассмотреть ИИ через теорию Л. И. Петражицкого, он займёт то же место, что и юридические лица в концепции учёного. ИИ и его юниты, точно так же, как и ЮЛ, в структуре правоотношений полноценными субъектами права в классическом понимании быть не могут. При этом, необходимо исходить

из принципа антропоцентричности права.

К сожалению, пока ещё ни один нормативно-правовой акт не дал ответ на вопрос, кто является субъектом права в информационном обществе, в том числе в социальных отношениях с использованием искусственного интеллекта. В настоящее время, подлинных субъектов правоотношений в информационном и цифровом обществе, кроме как человека, выявить не получается. При этом профессор А. А. Васильев пишет, что в настоящее время ИИ не является не только субъектом, но и объектом права, в классическом понимании, быть не может⁴. А продукты информационного общества, в том числе с использованием технологии ИИ, могут выполнять заданные алгоритмы и без признания их субъектами права, они выступают средством реализации потребностей человека.

Таким образом, нельзя забывать, что правоотношение выступает, по утверждению С. С. Алексеева, главным средством, с помощью которого юридические нормы действуют и реализуются⁵. Данный факт подчёркивает важность правоотношения и его структуры, а субъекту праву отведена роль проводника теории права в реальность.

¹ Габов А. В. Правосубъектность: традиционная категория права в современную эпоху // Вестник СГЮА. 2018. № 2 (121). С. 96–110.

² Павлов В. И. Учение о человеке в психологической концепции права Л. И. Петражицкого и в современной антропологии права // Правоведение. 2017. № 6 (335). С. 87–103.

³ Петражицкий Л. И. Теория права и государства в связи с теорией нравственности в 2 ч. Часть 2. Москва: Издательство Юрайт, 2019. 237 с.

⁴ Печатнова Ю. В., Васильев А. А. Место искусственного интеллекта среди элементов состава правоотношения // Цифровое право. 2020. № 1 (4). С. 74–83.

⁵ Алексеев Н. Н. Основы философии права. С. 131–134.

Поэтому необходимо чётко и | и правоотношений, которыми в
выверенно определять субъектов права | настоящее время является человек.

Список литературы

1. Алексеев С. С. Общая теория права: учебник. 2-е изд., перераб. и доп. М.: Проспект, 2009. 576 с.
2. Габов А. В. Правосубъектность: традиционная категория права в современную эпоху // Вестник СГЮА. 2018. № 2 (121). С. 96–110.
3. Павлов В. И. Учение о человеке в психологической концепции права Л. И. Петражицкого и в современной антропологии права // Правоведение. 2017. № 6 (335). С. 87–103.
4. Петражицкий Л. И. Теория права и государства в связи с теорией нравственности в 2 ч. Часть 2. Москва: Издательство Юрайт, 2019. 237 с.
5. Печатнова Ю. В. Место искусственного интеллекта среди элементов состава правоотношения / Ю. В. Печатнова, А. А. Васильев // Цифровое право. 2020. № 1 (4). С. 74–83.

Natalia E. Kovalenko
Graduate student,
Altai State University
(Barnaul, Russian Federation)
Kovalenkorub5@gmail.com

ARTIFICIAL INTELLIGENCE: THE RIGHT TO PARTICIPATE IN LEGAL RELATIONS AS A SUBJECT

Abstract: The article deals with the attribution of artificial intelligence and its units to the category of legal subjects, including the subjects of legal relations. L.I. Petrazhitzky's theory for comparative analysis of AI and UL position is given, as they are not classical categories from the viewpoint of human subject of law. The conclusion about the truth of the subject of law, which is directly human, is made.

Keywords: artificial intelligence, the subject of law, the subject of legal relations, legal relations, the theory of law, anthropocentricity of law.

Берсенеv Евгений Валерьевич
Курсант,
Уральский юридический институт МВД России
(г. Екатеринбург, Российская Федерация)
berevgArt@mail.ru

Научный руководитель – Р. С. Хамидуллин, кандидат юридических наук,
начальник кафедры оперативно-розыскной деятельности

ОСОБЕННОСТИ ПРОВЕДЕНИЯ ОРМ ПО ВЫЯВЛЕНИЮ НЕЗАКОННЫХ ТРАНЗАКЦИЙ И ДЕЯТЕЛЬНОСТИ, СВЯЗАННЫХ С ЯВЛЕНИЕМ «ВЕБКАМ»

Аннотация: Автор исследует финансовые аспекты, а также анализируется возможность проведения некоторых оперативно-розыскных мероприятий в отношении незаконной деятельности, связанной с явлением «вебкам»: наличие несовершеннолетних, вовлеченных в вебкам-студии, легализация доходов, полученных преступным путем, трансляция детской порнографии. Автор приходит к выводу о целесообразности внедрения технологических новшеств в деятельность правоохранительных органов, а также применению новых законодательных трендов для превенции преступности.

Ключевые слова: явление «вебкам», оперативно-розыскные мероприятия, несовершеннолетние, IT-сфера, криптовалюта.

Для цитирования:

Берсенеv Е. В. Особенности проведения ОРМ по выявлению незаконных транзакций и деятельности, связанных с явлением «вебкам» // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 200–205.

Современная форма построения экономических отношений построена на рыночной структуре, направленной на глобальный, мировой рынок, в рамках которого цифровизация общества дала резкий скачок в количественном предложении товаров и услуг. С начала 2000-х годов мир познакомился с бытовым использованием видеосвязи, ограниченными пределами зоны доступа интернета. С

диджитализацией мира пределы стали практически безграничными, следовательно и связь «продавец – покупатель» позволила реализовывать коммерческий продукт в практически любых географических данных.

Явление «вебкам» соединило в себе несколько таких составляющих, синтезировав в себе анонимизированное, дистанционное, глобализированное, коммерчески эффективное, не облагаемое налогами,

декриминализированное явление. Изучив данные исследования «Отношение уголовного закона Российской Федерации к явлению «вебкам», выделяем главную особенность, что даже при отсутствии состава преступления, так или иначе оно несет общественную опасность, обусловленную как экономической неподконтрольностью, так и возможным вектором развития для увеличения коммерческой эффективности (то есть привлечение детей, использование вымогательств и иных изобличающих работников данной сферы вещей).¹

В целом явление «вебкам» (вебкам моделинг) – определенный вид предоставления услуг с целью получения прибыли, посредством трансляции эротического или порнографического контента в онлайн-режиме с элементами общения, где модель, оказывающая услугу, не может видеть пользователя. Однако разнообразие в формах работы, организации и уровня финансирования крайне вариативны, таким образом отклонения от понятия допустимы, но при соблюдении общей содержательной стороны².

В контексте данного исследования, рассмотрены вопросы получения денежных средств, их конвертации и вывода, а также

вопросы юридической оценки данных действий.

Работа модели, как ранее упоминалось, организуется через специальные сайты (Chaturbate.com, streamate.com, livejasmin.com, Flirt4free.com, stripchat.com, xlove.com и другие). Технически, к примеру, Chaturbate – платформа, предоставляющая определенную вычислительную инфраструктуру, которая позволяет третьим лицам разрабатывать, настраивать и запускать различные виды приложений через интерфейс прикладного программирования (API). Как правило, модель ведёт трансляцию одновременно на нескольких сайтах, с целью повышения охвата аудитории. Модель, работающая в вебкам-студии, транслируется на 5–7 сайтах, а работающая на себя, на 1–3. Именно на таких сайтах происходит продажа услуг и их последующая оплата, а именно мемберы за время, проведенное в «приватных чатах», или за определенные действия со стороны вебкам-моделей переводят на внутриплатформенный кошелек определенное количество внутриплатформенной валюты («токены», «баксы», «коины»). Далее, через определенные промежутки времени, «периоды» происходит перевод уже конвертированных средств в доллары США или Евро.³

¹ Заирная М. М. Квалификация распространения порнографических видеоматериалов в режиме реального времени с использованием сети «интернет» // Уголовное право. 2015. № 6. С. 16–22.

² Берсенов Е. В. Отношение уголовного закона Российской Федерации к явлению

«вебкам» // Вопросы российской юстиции. 2021. № 15. С. 485–491.

³ Van Doorn N. A good hustle: the moral economy of market competition in adult webcam modeling / N. Van Doorn, O. Velthuis // Journal of Cultural Economy. 2018. № 11. P. 177–192. Accessed at: URL:

«Сток» внутренней валюты направляется на электронный кошелек, внутренняя политика которого позволяет принимать конвертированную валюту без проверки на способ или путь, которым были заработаны данные средства. Наиболее популярной платформой для этого является электронная платежная система «Ракхум», юридический адрес которого находится в Канаде.

В рамках независимости вебкам-сайтов разрабатывается и активно внедряется криптовалюта, которая позволит обойти ограничения, создаваемые банками и ЭПС. Использование технологии blockchain позволяет внедрять в денежный оборот криптовалюту Ethereum (Эфириум) в работу вебкам-сайтов. Данным технологическим обновлением занимается проект Spankchain, являющийся платежной системой нового поколения – децентрализованных онлайн-сервисов, основная цель которого во внедрении технологий, позволяющих совершать безопасные, а главное анонимные денежные переводы, в вебкам-индустрию^{4,5}. Фактически, говорится о создании независимой сферы, регулирование которой будет относительным и крайне трудоемким процессом.

Далее денежные средства перечисляются на валютный счет пользователя в местный банк в стране

пребывания для дальнейшего их обналичивания.

Проведение информационно-аналитической работы обусловлено необходимостью документирования событий и действий, выполняемых сотрудниками органов внутренних дел.

Первый этап состоит в выявлении факта противоправной деятельности относительно критериев квалификации, рассмотренных выше. Выявление происходит путем определения субъекта преступления, а также фактов преступления.

Особенности выявления и дальнейшего документирования проявляются в получении информации разными вариациями, предусмотренными оперативно-розыскными мероприятиями.

Прямой информационно-аналитический поиск релевантной и оперативной информации в сети «Интернет» на просторах площадок, названных в технической части.

Также менее масштабным, но конкретизированным является получение сведений от лиц ведущих негласное сотрудничество с органами внутренних дел. Привлечение к оперативно-розыскным мероприятиям администраторов, моделей и иных участников деятельности вебкам-студий позволяет сформировать целостную картину о противоправной деятельности отдельных субъектов, а также получить достаточную

<https://www.tandfonline.com/doi/full/10.1080/17530350.2018.1446183> (accessed: 01.03.2022).

⁴ Stone Z. How SpankChain, An X-Rated Blockchain, Wants To Be Porn Stars Go-To Cryptocurrency // Forbes Advertisement, 2017. URL: <https://www.forbes.com/sites/zarastone/2017/10>

/25/how-spankchain-an-x-rated-blockchain-plans-to-provide-pornstars-with-better-payment-plans/?sh=60ec13173659 (accessed: 01.03.2022).

⁵ Официальный сайт проекта SpankChain. URL: <https://spankchain.com/> (дата обращения: 02.03.2022).

доказательную базу как для возбуждения уголовного дела, сопровождения уголовного преследования, так и для предоставления доказывающих виновность фактов в суд во время судебного разбирательства. Таким образом, не требуется проведение сложной процедуры по подготовке и внедрению агентуры, ввиду их способностей главной задачей остается их поиск и вербовка⁶.

Достаточно редким случаем является информация, поступившая от родственников, соседей или самих вебкам-моделей, которые стали жертвами деанонимизации (раскрытия деятельности в вебкам-индустрии). Оперативная работа в таком случае сводится к стандартным процедурам и средствам проведения оперативно-розыскных мероприятий: осмотр места происшествия, т. е. в офисах-вебкам-студиях, выписки с банковских счетов моделей, администраторов и хозяев вебкам-студий, электронных систем по конвертированию цифровой валюты в реальные эквиваленты (обменники). Перед ОРМ ставятся следующие задачи:

1. Определение круга лиц, участвующих в деятельности «вебкам», особое внимание уделяется наличию несовершеннолетних, способы привлечения их к этой

деятельности и наличие фактов сексуальной эксплуатации⁷.

2. Способы расчета мемберов с вебкам-студией – использование зарубежной валюты / криптовалюты / иных аналогов, представляющих возможность их конвертирования в реальные денежные средства. Установление пути, т. е. использование специальных сайтов, выделение расчетных счетов на электронных платежных системах, рынки криптовалюты приравненные к ним обменники криптовалюты.

3. Проверка наличия каналов связи в случае согласованного транслирования детской порнографии посредством специальных сайтов. Таким каналами связи могут являться форумы на платформах-.onion, либо telegram-каналы и другие средства связи (социальные сети и иные мессенджеры).⁸

4. Установление IP адресов, либо, при наличии возможности, непосредственно лиц, приобретающих услуги вебкам-студий, распространяющих детскую порнографию обозначенным способом.

5. Сбор всех материальных носителей, а также получение доступа к «облачным» хранилищам, на которых могут содержаться материалы порнографического характера, с последующей привязкой записанного

⁶Жданов Ю. Н., Овчинский В. С. Кибермафия как объект оперативно-розыскного воздействия // Оперативно-розыскная деятельность в цифровом мире. 2021. С. 36–48.

⁷Смирных С. Е. Международное сотрудничество в борьбе с коррупцией как

гарантия предупреждения торговли детьми // Российская юстиция. 2020. № 12. С. 16–19.

⁸Рожкова М. А. Право в сфере Интернета: Сборник статей / ответ. ред. М. А. Рожкова. Москва: ООО «Издательство «СТАТУТ», 2018. 528 с.

материала к конкретным лицам, осуществляющим запись. Также осуществить привязку лиц к персональным компьютерам вебкам-студии.

Исследование явления «вебкам», проведенное в рамках данной работы, позволяет сделать выводы о целесообразном использовании правоохранительными органами инновационных внедрений и разработок. При этом использование новшеств российского законодательства (ввиду вступления в силу ФЗ «Об экспериментальных

правовых режимах в сфере цифровых инноваций в Российской Федерации» от 31.07.2020 № 258-ФЗ, на основании п. 4–5, ч. 2, ст. 1) закономерно продвигает идею о возможности внесения явления «вебкам» в правовую сферу как самостоятельного явления. Дополнительно стоит выделить методическое и технологическое совершенствование деятельности правоохранительных органов и их международное сотрудничество в рамках борьбы с организованными преступными организациями и «отмыванием» денег.

Список литературы

1. Берсенов Е. В. Отношение уголовного закона Российской Федерации к явлению «вебкам» // Вопросы российской юстиции. 2021. № 15. С. 485–491.
2. Жданов Ю. Н. Кибермафия как объект оперативно-розыскного воздействия / Ю. Н. Жданов, В. С. Овчинский // Оперативно-розыскная деятельность в цифровом мире. 2021. С. 36–48.
3. Зазирная М. М. Квалификация распространения порнографических видеоматериалов в режиме реального времени с использованием сети «интернет» // Уголовное право. 2015. № 6. С. 16–22.
4. Рожкова М. А. Право в сфере Интернета: Сборник статей / ответ. ред. М. А. Рожкова. Москва: ООО «Издательство «СТАТУТ», 2018. 528 с.
5. Смирных С. Е. Международное сотрудничество в борьбе с коррупцией как гарантия предупреждения торговли детьми // Российская юстиция. 2020. № 12. С. 16–19.
6. Van Doorn N. A good hustle: the moral economy of market competition in adult webcam modeling / N. Van Doorn, O. Velthuis // Journal of Cultural Economy. 2018. № 11. P. 177–192. Accessed at: URL: <https://www.tandfonline.com/doi/full/10.1080/17530350.2018.1446183>.
7. Stone Z. How SpankChain, An X-Rated Blockchain, Wants To Be Porn Stars Go-To Cryptocurrency // Forbes Advertisement, 2017. URL: <https://www.forbes.com/sites/zarastone/2017/10/25/how-spankchain-an-x-rated-blockchain-plans-to-provide-pornstars-with-better-payment-plans/?sh=60ec13173659>.

Evgeny V. Bersenev

Cadet,

Ural Law Institute of the Ministry of Internal Affairs of Russia
(Yekaterinburg, Russian Federation)

berevgArt@mail.ru

Scientific supervisor – R. S. Khamidullin, PhD (Law), Head of the Department of Operative-Search Activities

THE SPECIFICS OF CONDUCTING AN OPM TO IDENTIFY ILLEGAL TRANSACTIONS AND ACTIVITIES RELATED TO THE PHENOMENON OF «WEBCAM»

Abstract: The author explores the financial aspects, and also analyzes the possibility of carrying out some operational investigative measures in relation to illegal activities related to the phenomenon of «webcam»: the presence of minors involved in webcam studios, the legalization of proceeds from crime, the broadcast of child pornography. The author comes to the conclusion about the expediency of introducing technological innovations in the activities of law enforcement agencies, as well as the application of new legislative trends for the prevention of crime.

Keywords: the phenomenon of «webcam», operational search activities, minors, IT sphere, cryptocurrency.

УДК 34.09

Кошетьова Мария Денисовна

Студент,

Саратовская государственная юридическая академия

(г. Саратов, Российская Федерация)

koshetova.maria@gmail.com

Лубянкин Никита Романович

Студент,

Саратовская государственная юридическая академия

(г. Саратов, Российская Федерация)

nikita.lubiankin14.14.14@yandex.ru

Научный руководитель – Т. А. Савельева, кандидат юридических наук,
доцент кафедры арбитражного процесса

ЦИФРОВИЗАЦИЯ АДВОКАТУРЫ

Аннотация: В данной статье рассматривается развитие цифровизации в сфере адвокатской деятельности. Авторы опираются на мнения учёных, высказывают свою точку зрения. Выделяются положительные стороны использования информационных технологий в адвокатуре. Помимо этого, рассматриваются и проблемы в данной сфере.

Ключевые слова: цифровизация, адвокат, правовой акт, адвокатская деятельность, информационные технологии.

Для цитирования:

Кошетьова М. Д., Лубянкин Н. Р. Цифровизация адвокатуры // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 206–209.

В 2017 году Президент Российской Федерации утвердил Указ «О стратегии развития информационного общества в Российской Федерации», который стал толчком для развития информационно-коммуникационных технологий и внедрения их в различные сферы нашей жизни¹. В настоящее время

цифровизация меняет мир и неизбежно затрагивает сферу адвокатской деятельности. Особенно заметно это стало в момент пандемии COVID-19, когда большая часть работы адвокатов перешла в онлайн-режим.

Так, например, А. Н. Приженникова пишет, что благодаря цифровым технологиям адвокатура

¹ Указ Президента РФ от 9 мая 2017 г. №203 «О стратегии развития информационного

общества в Российской Федерации на 2017–2030 годы».

сегодня – это новые формы работы, новый качественный уровень². Разделяя указанную позицию, считаем, что значимость цифровизации в адвокатской деятельности проявляется ещё и в том, что адвокатура является одним из важнейших институтов в гражданском обществе и создана в целях обеспечения для граждан квалифицированной юридической помощи.

А. С. Советкина и А. В. Лошкарёв отмечают, что одним из первых и важнейших прорывов цифровизации можно считать компьютерную справочно-информационную систему «КонсультантПлюс»³. Нельзя не согласиться с этим, ведь её система оказала положительное влияние на все сферы юридической деятельности и на адвокатуру, в том числе. На 2022 год «КонсультантПлюс» содержит более 226 млн документов. Для адвоката данная система является незаменимым помощником при защите прав своего доверителя.

Ключевым моментом в развитии цифровизации можно назвать и такие информационные ресурсы как ГАС «Правосудие», «Гарант», «Картотека арбитражных дел» и др. Они включают в себя не только информацию по правовым актам, но и различные судебные решения, помогают осуществлять подачу электронных документов и отслеживать информацию о ходе рассмотрения дел. Это позволяет адвокату быстро и

эффективно производить подготовку к судебному заседанию, собирать необходимые документы и оставаться всегда в курсе последних изменений в законодательстве.

У цифровизации существует достаточно много плюсов, наиболее важными из которых представляются:

1. Упрощение таких процедур как подача судебных документов, адвокатских запросов.

2. Предоставление только действующих правовых актов.

3. Предоставление официальных сведений об адвокатах и адвокатских сообществах на сайте ФПА РФ в виде целостной базы, что защищает от мошеннических преступлений в сфере оказания адвокатских услуг.

4. Снижение финансовых затрат как для адвокатов, так и для самих доверителей.

5. Снижение временной нагрузки адвокатов.

6. Возможность следить за ходом рассмотрения дел.

Конечно, плюсов у цифровизации достаточно много, но есть и минусы, которые создают некоторые проблемы в данной сфере. Так, например, несмотря на существование в различных сферах юридической деятельности (у прокуратуры, судов) комплексных информационных систем, позволяющих организовать внутри- и межведомственное взаимодействие, в адвокатуре таковая отсутствует, хотя

² Приженникова А. Н. Цифровые технологии в практической деятельности адвоката // Образование и право. 2020. № 5. С. 223–226.

³ Советкина А. С., Лошкарёв А. В. Развитие цифровизации в сфере адвокатуры и

адвокатской деятельности: преимущества и возможные недостатки // Международный журнал гуманитарных и природных наук. 2020. № 9-2 (48). С. 195–199.

её создание упростило бы взаимодействие адвокатов с судебной системой, ведение бухгалтерии, а также подачу различных документов и запросов. В 2019 г. на Всероссийском съезде адвокатов впервые была предложена такая платформа, но она всё ещё находится на стадии разработки⁴. Однако уже сейчас можно прогнозировать, что она будет конфиденциальной, хорошо защищённой и удобной в использовании.

Помимо этого, проблемой выступает то, что не все хорошо владеют компьютерными технологиями, хотя, в настоящее время отсутствие знаний в данной сфере очень сильно усложняет работу в различных профессиях. Именно

поэтому следует вводить различные курсы по обучению в сфере компьютерных технологий, а также проводить консультации, которые будут касаться нововведений в данной отрасли.

Наконец, несмотря на удобство цифровых систем, нельзя забывать, что онлайн-коммуницирование снижает уровень доверия между доверителем и адвокатом.

Таким образом, мы видим, что цифровизация активно развивается в сфере адвокатуры, упрощая работу в данной отрасли. Однако ещё не решён ряд задач: этот процесс необходимо сделать организованным, разработать программы, которые будут учитывать разные уровни имеющейся у адвокатов цифровой компетентности.

Список литературы

1. Приженникова А. Н. Цифровые технологии в практической деятельности адвоката // Образование и право. 2020. № 5. С. 223–226.
2. Советкина А. С. Развитие цифровизации в сфере адвокатуры и адвокатской деятельности: преимущества и возможные недостатки / А. С. Советкина, А. В. Лошкарёв // Международный журнал гуманитарных и природных наук. 2020. № 9–2 (48). С. 195–199.

Maria D. Koshetova

Student,
Saratov State Law Academy
(Saratov, Russian Federation)
koshetova.maria@gmail.com

Nikita R. Lubyankin

Student,
Saratov State Law Academy
(Saratov, Russian Federation)

⁴ Старт КИС АР // ФПА РФ. 2019. 17 дек.
URL: <https://fparf.ru/news/fpa/start-kis-ar/> (дата обращения: 20.04.2022).

nikita.lubiankin14.14.14@yandex.ru

Scientific supervisor – T. A. Savelyeva, PhD (Law),
Associate Professor of the Arbitration Process Department

DIGITALIZATION OF THE LEGAL PROFESSION

Abstract: This article discusses the development of digitalization in the field of advocacy. The authors rely on the opinions of scientists, note their point of view. The positive aspects of the use of information technologies in the legal profession are highlighted. In addition, problems in this area are also being considered.

Keywords: digitalization, lawyer, legal act, advocacy, information technology.

УДК 34.096

Пащук Елена Олеговна

Студент,

Уральский государственный экономический университет

(г. Екатеринбург, Российская Федерация)

elenaand807@gmail.com

Научный руководитель – М. А. Задорина, кандидат
юридических наук, доцент кафедры конституционного и международного права

РАЗВИТИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ КАК УГРОЗА КОНФИДЕНЦИАЛЬНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация: Статья посвящена рассмотрению наиболее важных и актуальных вопросов развития процесса цифровизации. В частности, проанализированы проблемы защиты персональных данных пользователей при использовании различных цифровых технологий. Проведено сравнение аналитических данных утечек персональных данных пользователей за разные годы. Изучена зарубежная практика решения подобных вопросов. Предложены возможные решения проблем с учётом уровня правового развития и специфики общественных отношений в Российской Федерации.

Ключевые слова: персональные данные, конфиденциальность данных, цифровизация, цифровое право, правовое регулирование.

Для цитирования:

Пащук Е. О. Развитие цифровых технологий как угроза конфиденциальности персональных данных // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 210–216.

Современный мир характеризуется стремительным процессом цифровизации, охватившим все сферы общественной жизни. Многие склонны считать это началом четвёртой промышленной революции¹. Компании We Are Social и Hootsuite в прошлом году предоставили отчёт «Digital 2021», составленный на основе

данных Организации Объединённых Наций о количестве населения. Согласно нему, сеть Интернет используют около 60 % всего населения земного шара и ежегодно количество пользователей неуклонно возрастает. Необходимо отметить, что активными пользователями

¹ Schwab K. The Fourth Industrial Revolution // World Economic Forum, 2016.

социальных сетей являются 53,6 % или 4,2 млрд человек².

Всемирная паутина и цифровые технологии занимают важную роль в жизни большинства людей³. Процесс цифровизации оказал значительное влияние на изменение как бытовых, так и профессиональных аспектов жизнедеятельности общества⁴.

Внедрение инновационных технологий облегчило выполнение различных задач в таких сферах как образование⁵, медицина⁶, экономика⁷ и др. Например, всё большую популярность приобретают, так называемые «умные» устройства, имеющие доступ к сети Интернет и обменивающиеся данными между собой. Такая концепция получила название Интернет вещей или как её еще называют IoT. В последнее время Интернет вещей стремительно развивается, что способствует

изменению правоотношений между различными субъектами. Данный процесс перспективно влияет не только на экономический сектор, но и на другие сферы общественной жизни.

Широкое распространение социальных сетей, мессенджеров, маркетплейсов и цифровой торговли в целом также благоприятно влияет на государстве и обществе⁸. Если говорить о сделках купли-продажи посредством сети Интернет, то необходимо отметить, что с каждым годом они становятся всё более популярными. Режим самоизоляции, вызванный пандемией Covid-19, согласно данным исследовательского агентства «Data Insight», способствовал притоку не менее 10 миллионов новых покупателей в российскую онлайн-торговлю⁹.

Однако развитие информационных технологий имеет не

² Октябрьский статистический отчет по социальным сетям We Are Social // CPAGRAM. URL: <https://cpagram.ru/oktjabrskij-statisticheskij-otchet-po-socialnym-setjam-we-are-social/> (дата обращения: 01.05.2022).

³ Сексенбаев К. Информационные технологии в развитии современного информационного общества // Молодой ученый. 2015. № 24 (104). С. 191–194.

⁴ Коряковцева Н. А. Хрестоматия по информационной культуре. Сер. № 59. Серия Библиотекарь и время. XXI век. Моногр. М.: Либерея-Бибинформ, 2007. 144 с.

⁵ Задорина М. А. Некоторые проблемы цифрового обновления системы образования в условиях трансформации рынка труда // Достойный труд – основа стабильного общества: материалы XIII Международной научно-практической конференции. Екатеринбург: Изд-во УрГЭУ, 2021. С. 81–85.

⁶ Задорина М. А. Цифровизация здравоохранения и ее влияние на конституционное право на охрану здоровья и медицинскую помощь // Проблемы

взаимодействия публичного и частного права при регулировании цифровизации экономических отношений: материалы IV Международной научно-практической конференции. Екатеринбург: Изд-во УрГЭУ, 2021. С. 45–48.

⁷ Савоськин А. В. Цифровизация экономики как стратегическая цель развития России (правовой аспект) // Новая индустриализация России: экономика - наука – человек: сборник научных трудов VIII Уральских научных чтений профессоров и докторантов общественных наук. Екатеринбург: Изд-во УрГЭУ, 2021. С. 29–35.

⁸ Крупенский Н. А. Цифровая торговля: текущее состояние и перспективы развития в России и странах – членах ЕАЭС // Торговая политика. 2020. №1/21.

⁹ Пандемия ускорила темпы роста российской-онлайн торговли. // Газета РБК. URL: <https://www.rbc.ru/business/12/07/2020/5f0850989a794790e959424d> (дата обращения: 01.05.2022).

только положительные, но и отрицательные аспекты, например, такие, как:

- нарушение законных интересов пользователей,
- злоупотребление правами,
- пренебрежение обязанностями, связанное с наличием лакун в законодательстве.

Однако самой главной проблемой стремительной цифровизации, как считают учёные, является защита персональных данных пользователей в сети Интернет¹⁰.

Внедрение цифровых технологий трансформирует привычную концепцию защиты персональных данных. Используемые обществом цифровые технологии имеют функцию сбора частной информации, которая впоследствии может быть размещена в публичном доступе, так как данные устройства имеют доступ к сети Интернет. Проблема «утечки» личных данных приобретает всё более серьёзные масштабы с развитием цифровых технологий и IoT, в частности. Согласно статистике российской компании в области информационной безопасности «InfoWatch» в 2019 году во всём мире было похищено более 13 млрд записей персональных данных, а в 2020 году 100 млн записей персональных данных россиян и их

платёжной информации стали доступны третьим лицам.

В 2021 году произошла масштабная утечка персональных данных, в том числе номеров мобильных телефонов, биографические данные, даты и места рождения пользователей одной популярной социальной сети. В общей сумме пострадало около более 500 млн пользователей¹¹ из различных стран, включая Россию¹².

Необходимо отметить, что риск неправомерного доступа к персональным данным существует не только среди взрослого населения, но и среди несовершеннолетних. В 2017 году в открытом доступе оказались аудиозаписи разговоров, электронные адреса и пароли около 800 тысяч владельцев мягких игрушек фирмы «Cloud Pets», которые общаются с детьми и посредством сети Интернет отправляют данные на облачный сервер производителя, создавая потенциальную уязвимость для персональных данных несовершеннолетних.

Описанные выше случаи неправомерного завладения информацией не являются единичными. Стремительный и неизбежный характер развития средств онлайн коммуникации, цифровых технологий, в том числе и Интернета вещей, способствует увеличению

¹⁰ Шумекеева Г. Б. Защита персональных данных как одна из проблем современного мира // Право: современные тенденции: материалы VI Междунар. науч. конф. (г. Краснодар, октябрь 2018 г.). Краснодар: Новация, 2018. С. 47–49.

¹¹ Плюшевые игрушки подслушали разговоры пользователей по всему миру // Lenta.ru. URL: <https://lenta.ru/news/2017/03/01/cloudpets/> (дата обращения: 01.05.2022).

¹² Утечка данных пользователей // Газета РБК. URL: https://www.rbc.ru/technology_and_media/03/04/2021/60688ff9a7947cac2a65f28 (дата обращения: 01.05.2022).

ценности различного рода информации¹³. Это обуславливает значимость правового регулирования цифровых технологий, необходимых для защиты не только прав и свобод граждан, но и интересов всего общества и государства.

В соответствии с экспертными оценками, эффективное правовое регулирование цифровых технологий осложнено неопределённостью правового положения информации. Обращаясь к законодательной базе, необходимо отметить, что до 2006 года статья 128 Гражданского кодекса Российской Федерации рассматривала информацию в качестве объекта гражданских прав¹⁴. В настоящее время информация исключена из данного перечня. Однако исходя из анализа норм Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» можно сделать вывод, что данный законодательный акт позволяет рассматривать информацию в качестве объектов гражданских прав¹⁵.

Пункт 1 статьи 5 данного акта закрепляет следующее положение: «информация может являться объектом публичных, гражданских и иных правовых отношений». Вопрос об отнесении информации к объектам гражданских прав носит

дискуссионный характер. Однако легальное закрепление данного факта, способствовало бы эффективному развитию правоотношений, реализация которых возможна только под эгидой единых стандартов¹⁶.

Также статья 6 данного федерального закона разрешает процесс обработки персональных данных только при наличии письменного согласия лица. Однако обработка персональных данных без письменного согласия также будет признана легитимной, в случае если она необходима для защиты прав и законных интересов субъекта персональных данных. Многие цифровые технологии имеют не только своё физическое выражение, но и реализуются в сети Интернет, что может привести к завладению персональной информацией лицами, не имеющими к ней законного доступа.

Данные проблемы решаемы благодаря внесению точечных изменений в нормативно-правовые акты. Представляется возможным внесение поправок в Федеральный закон «Об информации, информационных технологиях и о защите информации».

Для решения вышеизложенных проблем возможно заимствование опыта других стран. В качестве примера можно рассмотреть принятый

¹³ Ковалева Н. Н. Проблемы и вызовы цифрового общества: тенденции развития правового регулирования цифровых трансформаций. Саратов: Изд-во ФГБОУ ВО «Саратовская государственная юридическая академия», 2020.

¹⁴ Гражданский кодекс Российской Федерации. Часть первая: федеральный закон

Российской Федерации от 30 ноября 1994 г. № 51-ФЗ // Российская газета. 2008.

¹⁵ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 2006. 29 июля.

¹⁶ Калинин А. С. Интернет вещей. Принципы, технологии, перспективы развития // Молодой ученый. 2019. № 2 (240). С. 341–342.

в США законодательный акт «SB-327», закрепляющий положения о безопасности устройств, имеющих подключение к всемирной паутине. Данный закон возлагает на разработчиков обязанность по обеспечению безопасности своих продуктов. Схожие положения содержит Британский кодекс «бытового интернета вещей». Однако необходимо помнить, что эффективное использование передовых решений зарубежных стран невозможно без учёта специфики существующей правовой системы государства.

Важно также иметь в виду, что проблема конфиденциальности персональных данных не является вызовом для одного государства, а носит международный характер. Как показывает практика, законодательное регулирование вопросов защиты персональных данных в рамках одной юрисдикции является неэффективным¹⁷. Среди учёных-правоведов всё чаще звучат предложения о необходимости чёткой регламентации данных правоотношений в рамках международного права.

Подводя итог, необходимо отметить, что эпоха всеобъемлющей цифровизации является подходящим временем для совершенствования правовой системы государства. Российская Федерация находится на пути развития законодательной регламентации информационной безопасности. Но большая часть НПА регулирует определённую узкую группу отношений, что формирует фрагментность правовой системы. При усилении правового регулирования в области защиты персональных данных пользователей необходимо соблюдение баланса, при котором борьба за безопасность персональных данных не создаст препятствий для развития и внедрения цифровых технологий. Исторический анализ свидетельствует о том, что процесс развития технологий опережал и будет опережать процесс правовой регламентации. Однако именно право является инструментом, необходимым для достижения равновесия между техническим прогрессом и социально-экономическим развитием общества и государства.

Список литературы

1. Задорина М. А. Некоторые проблемы цифрового обновления системы образования в условиях трансформации рынка труда // Достойный труд – основа стабильного общества: материалы XIII Международной научно-практической конференции. Екатеринбург: Изд-во УрГЭУ, 2021. С. 81–85.
2. Задорина М. А. Цифровизация здравоохранения и ее влияние на конституционное право на охрану здоровья и медицинскую помощь // Проблемы взаимодействия публичного и частного права при регулировании цифровизации

¹⁷ Исаков В. Б., Сарьян В. К., Фокина А. А. Правовые аспекты внедрения интернета

вещей // ИТ-СТАНДАРТ. 2015. № 4 (5). С. 9–16.

экономических отношений: материалы IV Международной научно-практической конференции. Екатеринбург: Изд-во УрГЭУ, 2021. С. 45–48.

3. Исаков В. Б. Правовые аспекты внедрения интернета вещей / В. Б. Исаков, В. К. Сарьян, А. А. Фокина // ИТ-СТАНДАРТ. 2015. № 4 (5). С. 9–16.

4. Калинин А. С. Интернет вещей. Принципы, технологии, перспективы развития // Молодой ученый. 2019. № 2 (240). С. 341–342.

5. Ковалева Н. Н. Проблемы и вызовы цифрового общества: тенденции развития правового регулирования цифровых трансформаций. Саратов: Изд-во ФГБОУ ВО «Саратовская государственная юридическая академия», 2020. С. 2–3.

6. Коряковцева Н. А. Хрестоматия по информационной культуре. Сер. № 59. Серия Библиотекарь и время. XXI век. Моногр. М.: Либерия-Бибинформ, 2007. 144 с.

7. Крупенский Н. А. Цифровая торговля: текущее состояние и перспективы развития в России и странах – членах ЕАЭС // Торговая политика. 2020. № 1/21. С. 2–3.

8. Савоськин А. В. Цифровизация экономики как стратегическая цель развития России (правовой аспект) // Новая индустриализация России: экономика - наука – человек: сборник научных трудов VIII Уральских научных чтений профессоров и докторантов общественных наук. Екатеринбург: Изд-во УрГЭУ, 2021. С. 29–35.

9. Сексенбаев К. Информационные технологии в развитии современного информационного общества // Молодой ученый. 2015. № 24 (104). С. 191–194.

10. Утечка данных пользователей // Газета РБК. URL: https://www.rbc.ru/technology_and_media/03/04/2021/60688ff99a7947cac2a65f28.

11. Шумекеева Г. Б. Защита персональных данных как одна из проблем современного мира // Право: современные тенденции: материалы VI Междунар. науч. конф. (г. Краснодар, октябрь 2018 г.). Краснодар: Новация, 2018. С. 47–49.

12. Schwab K. The Fourth Industrial Revolution // World Economic Forum, 2016. С. 2–3.

Elena O. Paschuk

Student,

Ural State University of Economics

(Yekaterinburg, Russian Federation)

elenaand807@gmail.com

Scientific supervisor – M. A. Zadorina, PhD (Law), Associate Professor of Department of constitutional and international Law

THE DEVELOPMENT OF DIGITAL TECHNOLOGIES AS A THREAT CONFIDENTIALITY OF PERSONAL DATA

Abstract: The article is devoted to the consideration of the most important and topical issues of the development of the digitalization process. In particular, the problems of protecting users' personal data when using various digital technologies are analyzed. Analytical data of leaks of personal data of users for different years have been carried out. The foreign practice of solving such issues has been studied in detail. Possible solutions to the problems are proposed, taking into account the level of legal development and the specifics of public and state relations in the Russian Federation.

Keywords: personal data, data privacy, digitalization, digital law, legal regulation.

УДК 343.1

Рукавишникова Галина Александровна
Курсант,
Уральский юридический институт МВД России
(г. Екатеринбург, Российская Федерация)
9089133977@mail.ru

Научный руководитель – А. В. Крысанов, кандидат юридических наук, доцент
кафедры оперативно-разыскной деятельности

К ВОПРОСУ ОБ ОБЕСПЕЧЕНИИ КОНСТИТУЦИОННОГО ПРАВА ГРАЖДАН НА ПОЛЬЗОВАНИЕ РОДНЫМ ЯЗЫКОМ В АСПЕКТЕ УГОЛОВНО-ПРОЦЕССУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация: Статья посвящена анализу текущего состояния проблем в области обеспечения права участников уголовного производства на пользование родным языком. Рассматривается возможность применения электронного переводчика, а также даются конкретные предложения по совершенствованию уголовно-процессуального законодательства.

Ключевые слова: права человека, электронный переводчик, следственные действия, язык судопроизводства, цифровые технологии, уголовный процесс.

Для цитирования:

Рукавишникова Г. А. К вопросу об обеспечении конституционного права граждан на пользование родным языком в аспекте уголовно-процессуальной деятельности // Технологии XXI века в юриспруденции: мат.-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 217–221.

Конституция Российской Федерации закрепляет основные права и свободы человека, а непосредственно потенциал их обеспечения и реализации рассматриваются уже не только в положениях Основного закона страны, но и в нормах

отраслевого законодательства. Так, ст. 26 Конституции РФ¹ закрепляет право человека на пользование родным языком, а ст. 18 УПК РФ², в целях его реализации, предусматривает возможность участников уголовного

¹ Конституция Российской Федерации // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 05.05.2022).

² Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-

ФЗ (ред. от 25.03.2022, с изм. от 19.04.2022) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 05.05.2022).

судопроизводства пользоваться помощью переводчика.

Говоря об обеспечении данного права, отметим, что на практике в России особые трудности возникают при поиске переводчиков с некоторых языков национальных меньшинств, например с цыганского, ингушского, даргинского, чеченского и др. Это вызвано большим разнообразием диалектов в языках, а также отсутствием лиц, способных осуществлять правильную интерпретацию понятийного аппарата уголовного судопроизводства.

Ещё одной проблемой в этой области выступает отсутствие у сотрудников правоохранительных органов возможности проверить на достоверность информацию, предоставляемую переводчиком. Разумеется, нормами уголовного законодательства предусмотрена ответственность за недостоверность переводимой информации, однако факт совершения такого правонарушения обнаружить достаточно сложно. Аналогичного мнения, о наличии данных проблем, придерживается и ряд учёных-правоведов, например В. А. Родивилина, О. П. Грибунов и др.³

В данном вопросе следует обратить внимание на существующую тенденцию постепенного внедрения на территории Российской Федерации цифровых технологий, способных самостоятельно решать поставленные

задачи, осуществлять сбор и обработку необходимых данных и выдавать уже готовый прогноз или результат. Одним из преимуществ их использования является экономия материальных и временных ресурсов, в связи с чем решение вышеперечисленных проблемных моментов нам видится в применении искусственного интеллекта и цифровых технологий, а именно технических средств, способных осуществлять точный и корректный перевод в целях обеспечения прав участников уголовного процесса.

Наиболее популярные и успешные инновации в области перевода предлагаются компаниями Deepl, Google и Яндекс – программы, обладая такими качествами как оперативность и качество, позволяют получать перевод данных с большинства существующих в мире языков. Все три программы способны распознавать фото- и аудио-информацию, однако отличием программы Deepl является возможность импортировать тексты из других приложений, например из документов в формате DOC и PDF, то есть не нужно копировать текст и вставлять его в программу, достаточно просто прикрепить файл, перевод которого необходимо осуществить (изменение самой структуры документа при этом не происходит)⁴.

Использование технических средств осуществления перевода в

³ Грибунов О. П., Родивилина В. А. Некоторые тактические особенности привлечения переводчика к участию в предварительном расследовании // Известия тульского государственного университета.

Экономические и юридические науки. 2014. № 3–2. С. 127.

⁴ Блог Deepl // Компания Deepl: официальный сайт. URL: <https://www.deepl.com/ru/blog> (дата обращения: 07.05.2022).

настоящее время не закреплено в законодательстве Российской Федерации, однако, в целях решения вышеперечисленных проблем, видится необходимым рассмотреть возможность дальнейшего совершенствования норм, регламентирующих использование электронного программного обеспечения по распознаванию и переводу речи участника процессуальных (следственных) действий с целью его перевода на русский язык.

Для иллюстрации эффективности применения таких средств перевода обратим внимание на опыт других стран. Так, в США для правоохранительных органов разрабатываются способы перевода устной речи. Принцип работы технологий заключается в следующем: на компьютер с помощью микрофона поступает голосовая информация, далее происходит перевод на выбранный язык, затем, уже интерпретированная информация озвучивается с помощью голосового помощника.

Подобные разработки успешно применяются на практике, поэтому считаем, что данный опыт возможен для применения в российском уголовном судопроизводстве⁵.

Как отмечалось выше, применение электронного переводчика можно рассматривать с двух сторон: с

одной – как альтернативу физическому лицу, производящему перевод, а с другой – как способ проверки такого лица. В обоих случаях уголовно-процессуальное законодательство требует определённых дополнений.

Первое из них связано с закреплением самого понятия «электронного переводчика» и требованиями, предъявляемыми к данной технологии, основным из которых следует назвать обязательное использование только сертифицированного программного обеспечения, то есть соответствующего техническим регламентам и документам по стандартизации, принятым или разрешённым на территории Российской Федерации. Поэтому, предлагаем, дополнить ст. 5 УПК РФ⁶ п. 63, следующего содержания:

«63) электронный переводчик – это техническое средство, применяемое следователем, дознавателем, прокурором, судом, обладающее сертифицированным программным обеспечением, а также возможностью распознавать и озвучивать речь человека в целях осуществления качественного перевода».

Такое дополнение, на наш взгляд, способно обозначить требования, предъявляемые к самой цифровой технологии, а также будет

⁵ Казначей И. В. Оптимизация условий предварительного расследования посредством использования электронного переводчика // Юридическая наука и правоохранительная практика. 2016. № 3 (37). С. 134.

⁶ Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 25.03.2022, с изм. от 19.04.2022) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 05.05.2022).

способствовать более чёткому осознанию смысла самого понятия.

Второе дополнение видится в закреплении права суда и стороны обвинения применять электронный переводчик в целях подтверждения правильности перевода, поэтому в ст. 59 УПК РФ, предлагаем внести ч. 1.1 следующего содержания:

«1.1. В целях проверки лица, осуществляющего перевод, следователем, дознавателем, прокурором и судом допускается применение электронного переводчика».

Данное нововведение позволит обеспечить права уголовно-преследуемого лица в полном объёме и исключить вероятность недостоверного или неточного перевода.

Последнее дополнение, которое представляется необходимым, непосредственно связано со случаями, когда своевременное нахождение лица, способного осуществить перевод крайне затруднено. Для разрешения такой ситуации предлагаем дополнить ст. 59 УПК РФ ч. 7 следующего содержания:

«7. В случае невозможности привлечения лица, свободно владеющего языком, знание которого необходимо для перевода, допускается применение электронного переводчика.

К числу таких случаев следует отнести обстоятельства когда:

а) прибытие лица, владеющего необходимым языком и способного осуществлять перевод, к месту

производства следственного действия не предоставляется возможным либо срок такого прибытия превышает 48 часов;

б) поиск лица, владеющего необходимым языком и способного осуществлять перевод, затруднён либо невозможен, либо не дал результатов в сроки, предусмотренные настоящим кодексом;

в) необходимо незамедлительное производство следственных либо иных процессуальных действий».

Полная замена физического лица, осуществляющего перевод на электронный переводчик, по нашему мнению, на данном этапе цифровизации государства, не является необходимым, поэтому дополнение в такой редакции видится наиболее целесообразным.

Подводя итоги, необходимо отметить, что, в соответствии с п. 5 ч. 2 ст. 381 УПК РФ, нарушение права уголовно-преследуемого лица на пользование помощи переводчика, относится к числу существенных нарушений уголовно-процессуального производства и может служить основанием для признания судебного решения недействительным. Именно поэтому считаем, что в целях реализации данного права, а также минимизации судебных издержек, использование цифровых технологий необходимо, кроме того, данная тенденция способна привести к существенной оптимизации деятельности правоохранительных органов.

Список литературы

1. Грибунов О. П. Некоторые тактические особенности привлечения переводчика к участию в предварительном расследовании / О. П. Грибунов, В. А. Родивилина // Известия тульского государственного университета. Экономические и юридические науки. 2014. № 3-2. С. 125–128.
2. Казначей И. В. Оптимизация условий предварительного расследования посредством использования электронного переводчика // Юридическая наука и правоохранительная практика. 2016. № 3 (37). С. 133–137.

Galina A. Rukavishnikova

Cadet,

Ural Law Institute of the Ministry of Internal Affairs of Russia
(Yekaterinburg, Russian Federation)
9089133977@mail.ru

Scientific supervisor – A. V. Krysanov, PhD (Law), Associate Professor of the
Department of operative-investigative activity

ON THE ISSUE OF ENSURING THE CONSTITUTIONAL RIGHT OF CITIZENS TO USE THEIR NATIVE LANGUAGE IN THE ASPECT OF CRIMINAL PROCEEDINGS

Abstract: The article is devoted to the analysis of the current state of problems in the sphere of ensuring the right of participants of criminal proceedings to use their native language. The possibility of using the electronic translator is considered; also, specific proposals for the improvement of criminal procedural legislation are given.

Keywords: human rights, electronic translator, investigative measures, language of court proceedings, digital technologies, criminal procedure.

Руф Владислав Сергеевич

Студент,

Уральский государственный университет

имени В. Ф. Яковлева

(г. Екатеринбург, Российская Федерация)

ruf.vlad-1988@yandex.ru

Научный руководитель – С. М. Суменков, кандидат экономических наук, доцент,
доцент кафедры предпринимательского права

ПЕРСПЕКТИВА РЕГУЛИРОВАНИЯ NFT

Аннотация: В статье характеризуется феномен невзаимозаменяемых токенов. Раскрывается сущность NFT, порядок создания, разновидности и варианты использования невзаимозаменяемых токенов. Приводятся подход к пониманию NFT как объекта гражданских прав. Формулируются выводы о возможности их правового регулирования.

Ключевые слова: NFT, невзаимозаменяемый токен, блокчейн, криптовалюта, цифровое пространство, объект права, гражданский оборот.

Для цитирования:

Руф В. С. Перспектива регулирования NFT // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 222–226.

Сегодня, с развитием науки и техники, с повсеместной глобализацией и компьютеризацией мировые тренды в экономике, политике и культуре постоянно претерпевают значительные изменения. С каждым годом создаётся всё большее число новых инструментов, моделей, программ и технологий, каждая из которых способна произвести переворот в той или иной сфере человеческой деятельности. Колоссальное развитие приобрели новшества, которые создаются и функционируют в цифровой среде с помощью сети

«Интернет». Так в 2021 году в мировой оборот очень быстро и в большом объёме зашли «non-fungible token» (невзаимозаменяемые токены; далее – NFT).

Обращаясь к средствам массовой информации, замечаем огромное количество статей, посвящённых продаже NFT за внушительные суммы денег, которые исчисляются в миллионах долларов. Например, NFT с названием «EVERYDAYS: THE FIRST 5000 DAYS» была продана за 69,3

миллиона долларов¹. Такие сделки неизбежно привлекают внимание не только экономистов, финансистов, аналитиков, но и юристов, так как постоянно растущая стоимость рынка NFT, которая уже на начало 2022 года по различным оценкам составляла 22–28 миллиардов долларов², непосредственно затрагивает экономический и соответственно гражданский обороты. Это порождает множество юридических и учётных проблем. Так, возникает вопрос о юридическом статусе NFT. В особенности, определение их правовой природы и соответственно правил оборота во многом осложнено отсутствием в отечественной и международной практике сформированного правового мнения об их сущности со стороны законодательных или судебных органов.

По мнению ряда отечественных исследователей, NFT представляет собой уникальный цифровой продукт, зашифрованный приёмами криптографии, который можно реализовать на цифровой платформе в киберпространстве³. Иностранные экономисты рассматривают NFT как единицу цифровой информации, хранящуюся в распределённом реестре

и являющуюся невзаимозаменяемой с иными цифровыми активами⁴. В данном определении NFT под «невзаимозаменяемостью» понимается невозможность их обмена на аналогичные активы. Отсюда можно заключить, что исключительной характеристикой нового вида токенов, которая была чётко подмечена экономистами всего мира, является их уникальность в цифровой сфере. NFT благодаря технологии блокчейн позволяют определить оригинальный цифровой след среди всего массива данных. По своей сути NFT обладает определённым водяным знаком, который позволяет отличить подлинный цифровой объект от его копии.

Эта же характеристика позволяет отграничить феномен NFT от другого основанного на блокчейне прорывного объекта современного мира, отражённого в цифровой среде, – криптовалюты. Например, биткоин полностью идентичен любому другому биткоину. Они служат цифровым аналогом валюты, в то время как ни один NFT не связан с какой-либо другой. Отсюда можно заключить, что стоимость каждого NFT, в отличие от каждого вида криптовалюты, формируется самостоятельно.

¹ Быковский А. Токены превращаются в люкс: 10 самых дорогих NFT-произведений на аукционах 2021 года. // Forbes.ru. 2021. 27 дек. URL: <https://www.forbes.ru/forbeslife/450565-tokeny-prevrasautsa-v-luks-10-samyh-dorogih-nft-proizvedenij-naaukcionah-2021-goda> (дата обращения: 20.04.2022).

² Воробей С., Бабенко С. 10 Самых дорогих NFT-картин на 2022 год. // Profinvestment.com. URL: <https://profinvestment.com/most-expensive-nft-paintings/> (дата обращения: 20.04.2022).

³ Блинова У. Ю., Рожкова Н. К., Рожкова Д. Ю. Феномен NFT (non-fungible tokens) как объекта бухгалтерского учета // Вестник ГУУ. 2021. № 11. С. 104.

⁴ Chohan U. W. Non-Fungible Tokens: Blockchains, Scarcity, and Value // Critical Blockchain Research Initiative (CBRI) Working Papers, 2021. 21 mar. Available at: URL: <https://ssrn.com/abstract=3822743>. DOI: <http://dx.doi.org/10.2139/ssrn.3822743> (accessed: 18.04.2022).

Продолжая рассматривать оборотоспособность NFT, обратимся к порядку их разработки. Первым этапом в этом процессе выступает создание какого-то объекта в материальном или цифровом пространстве, например, картины. Далее на торговой площадке производству присваивается уникальная запись в распределённом реестре блокчейн, и в последующем продаже, покупке, дарению подлежит именно запись в реестре, которая подтверждает владельца того или иного материального или виртуального объекта. Огромная популярность и востребованность NFT объясняется тем, что они могут использоваться при различных условиях. Торговая площадка вправе сама определять, сколько возможностей и прав будет у фактического обладателя токена: неисключительные права, которые оставляют возможность копировать произведение, наличие доли с продажи и перепродажи токена и другие⁵.

Бесспорно, новый вид уникальных токенов может быть отнесён к числу «виртуального имущества», под которым в научной литературе понимаются объекты нематериального мира, заключённые в цифру и представляющие прямой

экономический интерес субъектов права⁶. Однако из-за отсутствия нормативного закрепления данного понятия и его комплексности, видится необходимым определить к какому из объектов гражданских прав в соответствии со статьей 128 ГК РФ относится исключительно NFT.

NFT не может быть отнесён к категории вещей, так как сформировавшееся в научной литературе мнение гласит о том, что вещью может быть только объект материального мира, чем NFT не является. Также не представляется возможным приравнять NFT к интеллектуальной собственности, так как данные токены, как было отмечено, выступают всего лишь записью в реестре блокчейн и не подпадают ни под один из перечисленных в статье 1225 ГК РФ результатов интеллектуальной деятельности⁷. Данный перечень является закрытым, а соответственно, определение NFT как результата интеллектуальной деятельности возможно только при рассмотрении его в качестве уже указанного средства индивидуализации товара, однако неоднозначность определения характера самой записи, которая вносится о каждом NFT торговой площадкой на своё усмотрение, не

⁵ Емельянов Д. С., Емельянов И. С. Невзаимозаменяемые токены (NFT) как самостоятельный объект правового регулирования // Имущественные отношения в Российской Федерации. 2021. № 10 (241). С. 72.

⁶ Рожкова М. А. Цифровые активы и виртуальное имущество: как соотносится виртуальное с цифровым // Закон.ру. 2018. 13 июня. URL:

https://zakon.ru/blog/2018/06/13/cifrovye_aktiv_y_i_virtualnoe_imuschestvo_kak_sootnositsya_virtualnoe_s_cifrovym (дата обращения 01.04.2022).

⁷ Емельянов Д. С., Емельянов И. С. Невзаимозаменяемые токены (NFT) как самостоятельный объект правового регулирования // Имущественные отношения в Российской Федерации. 2021. № 10 (241). С. 73.

позволяет однозначно отнести токен к тому или иному средству.

NFT также не может быть включён в категорию цифровых прав, так как в соответствии со статьёй 141.1 ГК РФ к ним может быть отнесен сравнительно небольшой комплекс правомочий, распространяющихся на совокупность цифровых финансовых активов (цифровые права, включающие денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, права участия в капитале непубличного акционерного общества, право требовать передачи эмиссионных ценных бумаг, которые предусмотрены решением о выпуске цифровых финансовых активов)⁸ и включающий утилитарные цифровые права, направленные на законодательное регулирование краудфандинга⁹.

Основываясь на вышесказанном, можно сделать вывод, что NFT в наибольшей степени подпадает под категорию иного имущества, которое также состоит из множества элементов, в том числе имущественных и цифровых прав. Соответственно, из-за уникальности и неповторимости каждого NFT и правовых последствий, которые они влекут за собой для продавца и покупателя видится необходимым сначала дать внутреннюю классификацию невзаимозаменяемым токенам, а затем определить правовой режим каждого из определённых видов NFT с помощью их наложения на уже существующие объекты гражданских прав, так как современное законодательство уже обладает необходимым для этого потенциалом.

Список литературы

1. Блинова У. Ю. Феномен NFT (non-fungible tokens) как объекта бухгалтерского учета / У. Ю. Блинова, Н. К. Рожкова, Д. Ю. Рожкова // Вестник ГУУ. 2021. № 11. С. 103–109.

2. Быковский А. Токены превращаются в люкс: 10 самых дорогих NFT-произведений на аукционах 2021 года // Forbes.ru. 2021. 27 дек. URL: <https://www.forbes.ru/forbeslife/450565-tokeny-prevrasautsa-v-luks-10-samyh-dorogih-nft-proizvedenij-naaukcionah-2021-goda>.

3. Воробей С. 10 Самых дорогих NFT-картин на 2022 год / С. Воробей, С. Бабенко // Profinvestment.com. URL: <https://profinvestment.com> URL: <https://profinvestment.com/most-expensive-nft-paintings/>.

⁸ Федеральный закон от 31 июля 2020 года № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства акты Российской Федерации. 2020. № 31 (часть I). Ст. 5018.

⁹ Федеральный закон от 2 августа 2019 года № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства Российской Федерации. 2019. № 31. Ст. 4418.

4. Емельянов Д. С. Невзаимозаменяемые токены (NFT) как самостоятельный объект правового регулирования / Д. С. Емельянов, И. С. Емельянов // Имущественные отношения в Российской Федерации. 2021. № 10 (241). С. 71–76.

5. Рожкова М. А. Цифровые активы и виртуальное имущество: как соотносится виртуальное с цифровым // Закон.ру. 2018. 13 июн. URL: https://zakon.ru/blog/2018/06/13/cifrovye_aktivy_i_virtualnoe_imuschestvo_kak_sootnositsya_virtualnoe_s_cifrovym.

6. Chohan U. W. Non-Fungible Tokens: Blockchains, Scarcity, and Value // Critical Blockchain Research Initiative (CBRI) Working Papers, 2021. 21 mar. Available at: URL: <https://ssrn.com/abstract=3822743>. DOI: <http://dx.doi.org/10.2139/ssrn.3822743>).

Vladislav S. Ruf

Student,

Ural State Law University
named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
ruf.vlad-1988@yandex.ru

Scientific supervisor – S. M. Sumenkov, PhD (Economics), Associate Professor,
Associate Professor of the Department of Business Law

THE PERSPECTIVE OF NFT REGULATION

Abstract: The article characterizes the phenomenon of non-fungible tokens. The essence of NFT, the order of creation, varieties and use cases of non-fungible tokens are revealed. Various approaches to understanding NFT as an object of civil rights are given. Conclusions about the possibility of their legal regulation are formulated.

Keywords: NFT, non-fungible token, blockchain, digital space, legal object.

УДК 347.51.004.8

Сарксян Зоя Феликсовна

Студент,

Пермский филиал Национального исследовательского университета

«Высшая школа экономики»

(г. Пермь, Российская Федерация)

zfsarksyant@edu.hse.ru

Научный руководитель – О. С. Ерахтина, кандидат юридических наук, доцент,
доцент кафедры гражданского и предпринимательского права

ГРАЖДАНСКО-ПРАВОВАЯ ОТВЕТСТВЕННОСТЬ ЗА ДЕЙСТВИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД

Аннотация: В статье рассматривается риск-ориентированный подход к регулированию гражданско-правовой ответственности за вред, причинённый действиями искусственного интеллекта. Данный подход был положен в основу разработки проекта Регламента Европейского союза «О европейском подходе для искусственного интеллекта». В статье также анализируется классификация искусственного интеллекта по уровню риска причинения вреда. В соответствии с данной классификацией системы распределяются на три класса: чрезвычайно опасные, высокорисковые и системы с ограниченным и минимальным риском. Для каждого класса искусственного интеллекта определяется соответствующий ему режим гражданско-правовой ответственности.

Ключевые слова: искусственный интеллект, риск-ориентированный подход, класс рисковости, гражданско-правовая ответственность.

Для цитирования:

Сарксян З. Ф. Гражданско-правовая ответственность за действия искусственного интеллекта: риск-ориентированный подход // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 227–234.

Многие исследователи в области искусственного интеллекта придерживаются мнения, что традиционные институты, в том числе правовые, не отвечают тем вызовам, которые бросают обществу современные технологии. Искусственный интеллект, будучи

явлением фактически революционным, изменил представления о многих вещах, начиная с самой возможности человека создать подобное и заканчивая его же способностью до конца понять своё творение. И именно это открытие стало отправной точкой для исследования

многочисленных вопросов о том, как же будут урегулированы отношения «робот-человек» с этической, социологической, метафизической и др. точек зрения. Юридическая наука также не стоит в стороне. Отходя от классических институтов права, некоторые исследователи обращаются в том числе к смежным научным отраслям в попытках найти там эффективные механизмы для целей правового регулирования искусственного интеллекта. Так, одним из наиболее обсуждаемых подходов к регулированию гражданско-правовой ответственности за вред, причинённый действиями искусственного интеллекта, стал «риск-ориентированный» подход, получивший своё развитие, в частности, в стратегических документах Европейского Союза.

Основа «риск-ориентированного» подхода, как следует из названия, это система управления рисками, применяемая в менеджменте организаций, управлении проектами и других управленческих процессах. Обращение к данной системе при разработке механизма ответственности за действия искусственного интеллекта обусловлено тем, что эксплуатация технологий искусственного интеллекта на сегодняшний день так или иначе сопряжена со множеством рисков и упускать такой фактор из виду при разработке модели ответственности представляется

нецелесообразным. Следует рассмотреть подробнее данную концепцию.

Риск-менеджмент является неотъемлемой частью управленческих процессов в любой организации и предлагает множество концептуальных моделей и стандартов по регулированию рисков. Для целей исследования следует обратиться к Национальному стандарту по Менеджменту риска, в котором дано ёмкое определение понятию «риска» как «следствия влияния неопределённости на достижение поставленных целей»¹. Важно отметить, что в качестве указанного феномена могут классифицироваться события, наступление которых может повлиять как положительно, так и отрицательно на конечную цель. Обеспокоенность вызывают именно последние, и для устранения или минимизации их вредоносности в арсенале риск-менеджмента существует множество механизмов. Путём применения различных качественных и количественных методов оценки рисков специалисты устанавливают границы приемлемого риска и разрабатывают меры по реагированию на них. Что же этот механизм может дать праву для разработки модели ответственности за вред, причинённый действиями искусственного интеллекта? В первую очередь, это выявление самих рисков применения искусственного интеллекта, а также их оценку на

¹ ГОСТ Р ИСО 31000–2019. Менеджмент риска. Принципы и руководство // Электронный фонд правовых и нормативно-технических документов. URL:

<https://docs.cntd.ru/document/1200170125?section=text&marker=7D80K5> (дата обращения: 07.05.2022).

предмет приемлемости, что позволит классифицировать интеллектуальные системы для целей внедрения наиболее точного и эффективного правового регулирования в данной области.

Как уже упоминалось выше, риск-ориентированный подход активно исследуется учёными и экспертами Европейского Союза, вследствие чего он стал ядром некоторых европейских программных документов в области регулирования искусственного интеллекта. Так, он был положен в основу разработки проекта Регламента Европейского союза «О европейском подходе для искусственного интеллекта»². В указанном проекте системы искусственного интеллекта разделяются на 4 группы в зависимости от уровня риска причинения вреда.

1. Запрещённые системы искусственного интеллекта. К таковым относятся системы, способные манипулировать сознанием человека, исказить его поведение, причинять ему вред, дискредитировать и т. д. Соответственно, использование таких технологий недопустимо.

2. Высокорисковые системы искусственного интеллекта. В данную категорию входят системы, применяемые в области транспорта, образования, правоохранительной деятельности и др., а также системы, эквивалентные указанным по уровню риска. К ним, а также их владельцам и пользователям предъявляются

повышенные требования в области безопасности, учёта, прозрачности, предоставления информации и др. Кроме того, для эксплуатации таких технологий разработана особая система управления рисками, включающая несколько этапов оценки рисков: выявление и анализ, затем расчёт и оценка и, наконец, принятие мер по управлению выявленными рисками.

3. Системы с ограниченным риском. Ими могут быть, к примеру, чат-боты. В таком случае, на ресурсе будет лежать обязанность информировать пользователя о том, что он взаимодействует с искусственным интеллектом.

4. Системы с минимальным риском. В данную категорию попадают те технологии, которые не относятся к вышеперечисленным. К ним особых требований не предъявляется.

Таким образом, сформирован риск-ориентированный подход в целях регулирования сферы применения искусственного интеллекта в странах Европейского Союза. Вышеописанный проект представляет собой достаточно глубоко проработанную систему учёта и оценки рисков, с которыми может столкнуться общество при повсеместном внедрении искусственного интеллекта. Именно эта система должна быть взята в основу правовой регламентации отношений в сфере применения искусственного интеллекта, в частности, при решении вопроса о

² Regulation of the European Parliament and of the Council. Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts // EUR-Lex: EU Law portal. URL: [https://eur-](https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF)

[lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF) (accessed: 07.05.2022).

возможности его допуска на рынок. Это возможно только после соблюдения обязательных требований, описанных в документе, и предварительной оценки риска. Стоит отметить, что в зарубежном научном сообществе также существует повышенный интерес к риск-ориентированному подходу: учёными активно исследуются потенциальные угрозы, которые несут в себе технологии искусственного интеллекта.

Вышеописанная классификация в несколько изменённом виде может стать качественной основой для целей разработки модели ответственности за вред, причинённый действиями искусственного интеллекта. В частности, представляется возможным «наложить» описанную систему на имеющиеся в гражданском праве режимы ответственности для создания комплексного дифференцированного подхода к ответственности в сфере высоких технологий. Один из возможных вариантов такого «наложения» описан ниже.

Основой модели ответственности за вред, причинённый действиями искусственного интеллекта, будет являться классификация систем искусственного интеллекта. Выше приводилось описание деления технологий согласно проекту Регламента Европейского союза «О европейском подходе для искусственного интеллекта» в зависимости от уровня риска причинения вреда. Данный уровень определялся в зависимости от сферы применения, а также набора различных критериев, которые в совокупности оценивались экспертами и позволяли

соотносить ту или иную систему искусственного интеллекта с определённой степенью риска причинения вреда. Представляется, что именно данная классификация в несколько модифицированном и дополненном виде будет оптимальной для применения при разработке законодательных норм. В частности, дополнительно следует указать и характеристики искусственного интеллекта – высокоавтономный либо низкоавтономный, – так как это свойство может также предопределять степень рискованности её применения, а с ней и требовать установления соответствующего режима ответственности, который, в свою очередь, предлагается дифференцировать. Такая система позволит соотносить классы рисковости технологий с видами ответственности для каждой из них. Таким образом, для определения класса рисковости технологий искусственного интеллекта следует взять за основу сферы их применения, критерии для оценки риска, свойства системы, и в соответствии с ними определить режим ответственности за вред, причинённый определённым классом систем. Для каждого класса будет предусмотрен свой режим ответственности. Продемонстрируем это на примере.

Первый класс систем – чрезвычайно опасные технологии искусственного интеллекта. Прежде всего, это системы, применяемые в военном и оборонном секторе. В качестве критериев для определения таких видов систем могут выступать их сущностные характеристики – разрушение или уничтожение

заданной цели и др. В целом, учёные предлагают относить к данной категории любые системы, непосредственно причиняющие вред человеку. Можно предположить, что свойства автономности системы в данном случае не будут иметь значения, так как любые технологии такого типа представляют чрезвычайную опасность для людей. Их предлагается изъять из гражданского оборота.

Второй класс – высокорисковые системы. В него следует включить технологии искусственного интеллекта, применяемые в тех сферах, которые указаны для данного класса в проекте Регламента Европейского союза: биометрическая идентификация и категоризация физических лиц, управление и эксплуатация «критической» инфраструктуры (области дорожного движения, водо- и газоснабжения и др.), образование, трудоустройство и занятость населения, государственные услуги, правоохранительная деятельность, управление миграцией и пограничный контроль, отправление правосудия. Представляется, что заимствование данного перечня вполне соответствует принципам отечественного законодательства, в первую очередь в социальной сфере. С одной стороны, системы искусственного интеллекта в указанных сферах являются «социально-желательными», именно их развитие призвано отвечать общественно полезным целям, развивать данные отрасли, повышая в их рамках эффективность деятельности многих механизмов. С другой стороны, эти же технологии как

раз в силу их применения в социальной сфере, включающей взаимодействие с фактически неограниченным «неподготовленным» кругом лиц, могут причинить значительный вред в первую очередь жизни и здоровью человека.

В вышеописанном проекте Регламента Европейского Союза разработчиками предложены критерии для оценки эквивалентности риска причинения вреда, то есть идентификации системы как высокорисковой при условии того, что она не попадает под первую категорию. В частности, ими обозначены:

- 1) предполагаемое назначение системы;
- 2) степень «использованности» системы (предположительно, здесь подразумевается степень износа системы);
- 3) уже известные (документально подтверждённые) случаи причинения вреда такой системой;
- 4) потенциальный размер вреда или интенсивность неблагоприятного воздействия, которое может причинить система;
- 5) степень зависимости человека от результатов деятельности системы и возможность отказаться от её использования;
- 6) степень потенциальной уязвимости человека по отношению к системе из-за дисбаланса экономических и социальных обстоятельств;
- 7) степень обратимости результатов деятельности системы;
- 8) наличие в законодательстве эффективных мер по возмещению

причинённого вреда, по его предотвращению или минимизации.

Заимствование указанных критериев для оценки эквивалентности риска причинения вреда из проекта Регламента также представляется целесообразным. Вышеуказанные восемь критериев, предложенные в проекте европейского Регламента, вполне позволяют в конечном итоге ответить на вопрос о том, высок ли риск причинения вреда той или иной системой искусственного интеллекта. Возможна также регламентация определённых «пороговых» значений для каждого критерия с целью более точного разграничения видов систем. Например, высокорисковой системе может соответствовать 50% и выше степень «использованности» системы, два и более случая причинения вреда такой системой, потенциальный размер вреда более 100 000 рублей и т. д. Закрепление в виде конкретных показателей представляется возможным не для всех критериев, в частности, определить степень зависимости человека от результатов деятельности системы или степень потенциальной уязвимости человека по отношению к системе невозможно в числовых значениях, соответственно, их потребуется определять в зависимости от каждого конкретного случая.

Далее, в класс высокорисковых следует включить высокоавтономные системы искусственного интеллекта.

Следует отметить, что однозначные критерии для определения такой системы также отсутствуют, однако их разработка явно необходима, в том числе для целей законодательного регулирования. Такие критерии должны отталкиваться от свойств прозрачности и предсказуемости результатов работы системы, тем самым позволяя законодательно отграничить высокорисковые системы от других видов. Составить указанные критерии представляется возможным только с привлечением экспертов по отдельным видам технологий.

Представляется, что за действия вышеописанного класса систем должна быть предусмотрена строгая ответственность, которая видится одним из наиболее эффективных вариантов регулирования сферы именно высоких технологий³. Большинство учёных и экспертов склоняются к тому, что для высокорисковых систем искусственного интеллекта следует установить ответственность вне зависимости от вины⁴, что аргументируется не только свойствами их непредсказуемости и непрозрачности⁵, но также и фактически неограниченным кругом людей, с которыми потенциально будет взаимодействовать такая

³ Zech H. Liability for AI: public policy considerations // ERA Forum 22. 2021. P. 150.

⁴ Подходы к гражданско-правовой ответственности разработчика технологий искусственного интеллекта: на основе классификации технологий / А. О. Алексеев,

О. С. Ерахтина, К. С. Кондратьева [и др.] // Информационное общество. 2020. № 6. С. 53.

⁵ White J. M., Lidskog R. Ignorance and the regulation of artificial intelligence // Journal of Risk Research. 2021. DOI: 10.1080/13669877.2021.1957985.

система⁶. Правоведы справедливо отмечают, что строгая ответственность будет стимулировать субъектов, причастных к разработке и управлению высокорисковыми системами искусственного интеллекта совершенствовать их до тех пор, пока они не станут максимально безопасным, что также позволит повысить доверие пользователей к данным технологиям. Таким образом, для высокорисковых систем предлагается ввести строгую (безвиновную) ответственность.

Третий класс – системы с ограниченным и минимальным риском. Данные категории целесообразно объединить в силу возможности их сходного регулирования. К данному классу предполагается отнести чат-ботов, виртуальных помощников, умные дома, нейросети, генерирующие тексты песен, картины и др. Указанная категория представляется «остаточной», то есть системы, не вошедшие в первый и второй класс, автоматически будут отнесены к третьему. Касательно их свойств, они обычно являются «узкими», то есть имеют ограниченный функционал и задачи, соответственно, их возможность самообучаться также ограничена, а предсказуемость результатов, наоборот, высока. Следует, однако, учесть, что эти системы искусственного интеллекта имеют доступ к персональным данным, в силу чего к ним должны

предъявляться повышенные требования в области обработки и защиты личной информации. Тем не менее, такие технологии не создают высокий риск причинения вреда. За деятельности такого класса систем искусственного интеллекта следует предусмотреть виновную ответственность.

Таким образом, основу определения режима гражданско-правовой ответственности в сфере применения технологий искусственного интеллекта будет составлять дифференцированный подход, основанный на уровне риска применения различных видов технологий. Их классификация будет строиться на основании сфер применения конкретных видов технологий, характеристик автономности в зависимости от возможностей самообучения, свойств предсказуемости и прозрачности, а также критериев оценки риска для отдельных видов систем. В результате соотношения указанных характеристик искусственного интеллекта и режимов гражданско-правовой ответственности мы приходим к следующим выводам: чрезвычайно опасные системы искусственного интеллекта будут изъяты из гражданского оборота, за высокорисковые системы будет предусмотрена строгая ответственность, а за системы с ограниченным и минимальным риском – виновная ответственность.

⁶ Правовые аспекты использования искусственного интеллекта: актуальные проблемы и возможные решения / В. Б. Наумов, С. А. Чеховская, А. Ю. Брагинцев [и

др.]. М.: ИД ВШЭ, 2021. URL: <https://www.hse.ru/mirror/pubs/share/480106412.pdf> (дата обращения: 07.05.2022).

Список литературы

1. Подходы к гражданско-правовой ответственности разработчика технологий искусственного интеллекта: на основе классификации технологий / А. О. Алексеев, О. С. Ерахтина, К. С. Кондратьева [и др.] // Информационное общество. 2020. № 6. С. 47–57.
2. Правовые аспекты использования искусственного интеллекта: актуальные проблемы и возможные решения / В. Б. Наумов, С. А. Чеховская, А. Ю. Брагинец [и др.]. М.: ИД ВШЭ, 2021. URL: <https://www.hse.ru/mirror/pubs/share/480106412.pdf>.
3. White J. M. Ignorance and the regulation of artificial intelligence / J. M. White, R. Lidskog // Journal of Risk Research. 2021. DOI: 10.1080/13669877.2021.1957985.
4. Zech H. Liability for AI: public policy considerations // ERA Forum 22. 2021. P. 147–158.

Zoya F. Sarksyian

Student,

National Research University Higher School of Economics – Perm

(Perm, Russian Federation)

Zfsarksyian@edu.hse.ru

Scientific supervisor – O. S. Erahtina, PhD (Law), Associate Professor,
Associate Professor of the Department of Civil and Business Law

CIVIL LIABILITY FOR ACTIONS OF ARTIFICIAL INTELLIGENCE: A RISK-BASED APPROACH

Abstract: The article discusses a risk-based approach to the regulation of civil liability for damage caused by the actions of artificial intelligence, which became the basis of the European Union draft «Regulation on a European Approach for Artificial Intelligent». The authors investigate the classification of artificial intelligence according to the level of risk of causing harm. As a result, artificial intelligence systems are divided into three classes: extremely dangerous, high-risk, and systems with limited and minimal risk. For each of the classes of systems is determined the appropriate mode of civil liability.

Keywords: artificial intelligence, risk-based approach, risk class, civil liability.

УДК 347.2.3

Соколова Анастасия Юрьевна

Студент,

Сибирский Государственный Университет

Путей и Сообщения

(г. Новосибирск, Российская Федерация)

stasy.sokolova@icloud.com

Научный руководитель – С. В. Матияшук, доктор юридических наук, профессор
кафедры гражданско-правовых дисциплин

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОХРАНЫ ПРАВ СОБСТВЕННОСТИ НА РЕЗУЛЬТАТЫ ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация: В условиях интенсивного экономического развития Российской Федерации, важное значение приобретает гражданско-правовой оборот интеллектуальной собственности, которая выступает необходимым элементом деятельности человека в социально-экономической, духовной и политической сферах. Осознание этого и использование интеллектуальной собственности людьми в качестве важного преимущества при решении личных, коммерческих, политических, военно-политических и других вопросов способствовало повышению её роли и значения в качестве необходимого ресурса развития любой социальной группы. В статье детально анализируются особенности правового регулирования охраны прав собственности на результаты интеллектуальной деятельности.

Ключевые слова: интеллектуальные права, интеллектуальная собственность, результаты интеллектуальной деятельности (РИД), авторские права, Федеральная служба по интеллектуальной собственности (Роспатент).

Для цитирования:

Соколова А. Ю. Правовое регулирование охраны прав собственности на результаты интеллектуальной деятельности // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 235–239.

Интеллектуальная
собственность – собственность на
результаты интеллектуальной
деятельности; интеллектуальный
продукт, входящий в совокупность

объектов авторского и
изобретательского права¹.

Согласно Гражданскому
Кодексу Российской Федерации,
результатами интеллектуальной

¹ Гражданское право в 2 т. Т. 2: учебник / С. С. Алексеев, О. Г. Алексеева, К. П. Беляев [и

др.]. 3-е изд., перераб. и доп. М.: Статут. 2018. С. 578.

деятельности и приравненными к ним средствами индивидуализации юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана (интеллектуальной собственностью), являются:

- 1) произведения науки, литературы и искусства;
- 2) программы для электронных вычислительных машин (программы для ЭВМ);
- 3) базы данных;
- 4) исполнения;
- 5) фонограммы;
- 6) сообщение в эфир или по кабелю радио- или телепередач (вещание организаций эфирного или кабельного вещания);
- 7) изобретения;
- 8) полезные модели;
- 9) промышленные образцы;
- 10) селекционные достижения;
- 11) топологии интегральных микросхем;
- 12) секреты производства (ноу-хау);
- 13) фирменные наименования;
- 14) товарные знаки и знаки обслуживания;
- 14.1) географические указания;
- 15) наименования мест происхождения товаров;
- 16) коммерческие обозначения.

Право интеллектуальной собственности — законное право юридического или физического лица на владение авторскими правами, патентами, торговыми марками, связанные с конкретным товаром или

процессом.

Интеллектуальная собственность является нематериальным объектом права собственности. Поэтому охрана прав на объекты интеллектуальной собственности имеет свою специфику. Основными способами защиты в данном случае являются: выдача автору или другому субъекту права интеллектуальной собственности охранного документа: патента или свидетельства; авторское право; коммерческая тайна.

Правовое регулирование охраны прав на объекты интеллектуальной собственности в Российской Федерации осуществляется на основании Гражданского Кодекса Российской Федерации (части четвертой). Его существо состоит в том, что автор или другое признанное законом лицо получает от государства исключительные права на созданный объект интеллектуальной собственности на определённый (в законе) период времени². Эти права подтверждаются охранным документом, который выдаётся собственнику объекта интеллектуальной собственности и предоставляет право на защиту со стороны государства. Это даёт собственнику возможность раскрыть содержание своего объекта интеллектуальной собственности для всех лиц, чтобы они получили возможность использовать его на законных основаниях, т. е. по разрешению автора с обязательным

² Ивлиев Г. П., Егорова М. А. Обеспечение правовой охраны результатов интеллектуальной деятельности и

коммерциализации прав на них в ЕАЭС // Lex Russica. 2021. Т. 74, № 11. С. 14.

отчислением ему вознаграждения за разрешение на использование. Именно поэтому охрана, которая предоставляется интеллектуальной собственности государством, способствует увеличению числа изобретений и рационализаторских предложений, распространению новых идей, материалов, технологий, развитию научно-исследовательской деятельности, а в итоге – техническому и общественному прогрессу.

Охрана прав на объекты интеллектуальной собственности является действенным механизмом в плане защиты от недобросовестной конкуренции. Если бы такой охраны не было, то собственник объекта интеллектуальной собственности вместо дополнительной прибыли от его использования приобретал только убытки, ведь процесс создания (разработки) объекта интеллектуальной собственности требует значительных материальных затрат. Недобросовестные конкуренты в таких условиях могут «позаимствовать» идею на стадии, когда она уже готова к промышленному использованию. В этом случае они получают преимущество, поскольку не расходовали средства на стадии создания. Поэтому их продукция будет более дешёвой и вследствие этого – более конкурентоспособной.

Изобретатель, работодатель или правопреемник изобретателя или работодателя могут принять различные варианты решений относительно правовой охраны изобретения (полезной модели):

- сохранять конфиденциальность информации,

согласуясь с нормами законодательства о коммерческой тайне;

- сделать изобретение общедоступным без получения патента (путём демонстрации его на выставках, издания статей, монографий);

- получить патент на изобретение или полезную модель.

Охрана прав на объекты интеллектуальной собственности опирается на следующие принципы:

1. Охраноспособности. Он означает, что объект правовой охраны должен соответствовать указанным в законе требованиям (изобретение должно быть новым, иметь изобретательский уровень и являться промышленно применимым).

2. Признания за правообладателем исключительного права на объект права интеллектуальной собственности.

3. Соблюдения прав не только собственников права, но и действительных разработчиков (авторов, изобретателей).

4. Соблюдения баланса интересов собственников прав, с одной стороны, и общества – с другой, – путём ограничения монополии на объект права, например через установление разумного срока действия охранного документа.

Каждая страна осуществляет охрану прав на объекты интеллектуальной собственности самостоятельно. Если заявитель желает получить правовую охрану в других странах, он должен зарегистрировать своё право в каждой из этих стран. Однако международная охрана прав на объекты интеллектуальной собственности

призвана облегчить эту процедуру.

Международная правовая охрана объектов промышленной собственности предусматривает охрану изобретений, знаков (товарных знаков и знаков обслуживания), промышленных образцов и борьбу с недобросовестной конкуренцией. В 1983 г. была подписана Парижская конвенция по охране промышленной собственности, которая нередко пересматривалась, в результате чего каждый раз принимался Акт пересмотра Парижской конвенции.

Положения Парижской конвенции можно разбить на четыре основные категории³.

1. Первая содержит нормы материального права, которые гарантируют основное право, известное как право национального режима в каждой из стран членов.

2. Вторая устанавливает ещё одно основное правило, известное как право приоритета.

3. Третья определяет целый ряд общих норм в области материального права.

4. Четвертая формулирует административные рамки, установленные в целях реализации Конвенции, и включают

заключительные положения.

Своевременная правовая охрана и квалифицированное использование объектов интеллектуальной собственности является в наши дни необходимым условием успешного выхода на рынок и эффективного хозяйствования. Ведь практически любая современная технология базируется на изобретениях, удачный дизайн изделия обеспечивает спрос, а зарегистрированный товарный знак защищает от подделок и недобросовестной конкуренции.

Существующая в Российской Федерации государственная система охраны интеллектуальной собственности позволяет каждому физическому и юридическому лицу достаточно эффективно защищать и использовать плоды интеллектуального труда.

Правоотношения в этой области регулируются целым рядом законов и нормативных актов, без основательного знания которых, равно как и многих других, практических, вопросов получить надежную правовую охрану и компетентно использовать интеллектуальную собственность едва ли возможно.

Список литературы

1. Гражданское право в 2 т. Т. 2: учебник / С. С. Алексеев, О. Г. Алексеева, К. П. Беляев [и др.]. 3-е изд., перераб. и доп. М.: Статут. 2018. 672 с.
2. Ивлиев Г. П. Обеспечение правовой охраны результатов интеллектуальной деятельности и коммерциализации прав на них в ЕАЭС / Г. П. Ивлиев, М. А. Егорова // Lex Russica. 2021. Т. 74, № 11. С. 9–16.

³ Holyoak J., Torremans P. Intellectual Property Law. London; Edinburg; Dublin: Butterworths,

1998. P. 313.

3. Holyoak J. Intellectual Property Law / J. Holyoak, P. Torremans. London; Edinburg; Dublin: Butterworths, 1998. 596 p.

Anastasia U. Sokolova
Student,
Siberian State University of
Railways and Communications
(Novosibirsk, Russian Federation)
stasy.sokolova@icloud.com

Scientific supervisor – S. V. Matiyashchuk, Doctor of Law, Professor of the
Department of Civil law disciplines

LEGAL REGULATION OF THE PROTECTION OF PROPERTY RIGHTS TO THE RESULTS OF INTELLECTUAL ACTIVITY

Abstract: Under the conditions of intensive economic development of the Russian Federation, the civil legal turnover of intellectual property, which is a necessary element of human activity in the socio-economic, spiritual and political spheres, acquires great importance. The awareness of this and the use of intellectual property by people as an important advantage in solving personal, commercial, political, military and other issues has increased its role and importance as a necessary resource for the development of any social group. The article analyzes in detail the peculiarities of the legal regulation of the protection of property rights to the results of intellectual activity.

Keywords: intellectual rights, intellectual property, results of intellectual activity (RIA), copyrights, Federal Service for Intellectual Property (Rospatent).

Цветкова Анна Денисовна

Студент,

Уральский государственный юридический университет

им. В. Ф. Яковлева

(г. Екатеринбург, Российская Федерация)

at@crimlib.info

Научный руководитель – Д. В. Бахтеев, кандидат юридических наук, доцент
доцент кафедры криминалистики

ПРАВОВЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ КЕЙЛОГГЕРОВ

Аннотация: В статье раскрывается сущность кейлоггеров, даётся характеристика каждому их виду. Также рассматриваются возможные причины негативного отношения к данной технологии. Описывается полезная информация, которую можно получить с помощью кейлоггеров, и приводятся модели их практического применения в сфере трудовых отношений, уголовного и гражданского процессов, что сопровождается иллюстрированием ситуаций, где рассматриваемая технология незаменима. В конце описываются существующие на настоящий момент помехи для широкого внедрения кейлоггеров и обосновывается необходимость их преодоления путём дальнейших научных разработок по предложенной теме.

Ключевые слова: кейлоггер, компьютерный почерк, идентификация исполнителя текста, контроль рабочих процессов, аутентификация пользователя, контроль сетевого контента.

Для цитирования:

Цветкова А. Д. Правовые аспекты применения кейлоггеров // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 240–247.

В середине прошлого века появились кейлоггеры (они же перехватчики клавиатуры), которые многими из знакомых с данной технологией воспринимаются единственно в качестве устройств для слежки и похищения персональных

данных¹. Представляется, что такая позиция связана с недостаточным уровнем просвещения по данному вопросу, поэтому в настоящей работе мы поставили перед собой цель описать возможную пользу от применения кейлоггеров в различных

¹ Клавиатурные шпионы или как клавиатура может предать вас // Новости мира IT: блог на платформе «Дзен». 2019. 11 окт. // URL: https://zen.yandex.ru/media/it_news/klavi

aturnye-shpiony-ili-kak-klaviatura-mojet-predat-vas-5da04457ba281e00b3fa7a4d (дата обращения: 10.11.2021).

областях человеческой деятельности, а также предложить модели правового регулирования использования рассматриваемой технологии в отдельных сферах.

Под кейлоггерами (keylogger) принято понимать программно-аппаратные средства захвата показателей компьютерного почерка человека, в том числе времени и силы нажатия на клавиши². Они бывают трёх видов: программа; аппаратный блок, непосредственно внедрённый в клавиатуру или подключенный как внешний модуль^{3,4}; вибро-акустический улавливатель. Рассмотрим каждый подробнее.

Компьютерные программы, которые после установки и настройки становятся невидимыми для пользователя и большинства антивирусов, фиксируют любой набираемый текст и каждое нажатие клавиш (как символьных, так и служебных); посещённые сайты; время включения/выключения отдельной программы и ПК в целом; документы, отправленные на распечатку; также они способны делать снимки экрана в соответствии с заданными параметрами и сохранять скопированную в буфер обмена информацию. Далее все собранные сведения формируются с настроенной

регулярностью в читаемый человеком (то есть расшифрованный) отчёт и направляются на почту, сохраняются в сетевом окружении (на связанных с пользовательским устройствах) или передаются с помощью сетевых протоколов (например, FTP или SSH)⁵. Следует указать, что современные системы безопасности, встроенные в операционную систему, не позволяют установить программный кейлоггер человеку с низкой компьютерной грамотностью, хотя в свободном доступе их находится не мало.

Второй вид – аппаратные кейлоггеры – представляют собой внешние подключаемые к клавиатуре и компьютеру или встраиваемые в клавиатуру устройства, остающиеся незамеченными антивирусной защитой компьютера и считывающие все нажатия на клавиши, сохраняя информацию в собственную память, что делает их отчасти похожими на банкоматные скиммеры. Таким образом, доступ к собранной информации возможен только после физического обращения к устройству, однако некоторые современные кейлоггеры предусматривают системы

² Herley C., Florencio D. Microsoft Research How To Login From an Internet Cafe Without Worrying About Keyloggers // Symposium on Usable Privacy and Security (SOUPS). 2006. july. URL: <https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/soups06.pdf> (дата обращения: 09.11.2021).

³ Design and Evaluation of a Pressure-Based Typing Biometric Authentication System / W. Eltahir, M. Salami, A. Ismail, W. Lai //

EURASIP Journal on Information Security. 2008. Vol. 14.

⁴ Grabham N., White N. Use of a novel keypad biometric for enhanced user identity verification // Instrumentation and Measurement Technology Conference Proceedings, IMTC 2008. IEEE, 2008. P. 12–16.

⁵ Обзор клавиатурных шпионов: лучшие кейлоггеры // Журнал «Хакер». 2006. 4 дек. URL: <https://xaker.ru/2006/12/04/35563/> (дата обращения: 09.11.2021).

передачи данных по Wi-Fi⁶. Чаще всего они выглядят как небольшие устройства, подобные флеш-картам, подключаемым через USB или COM разъёмы. Такие кейлоггеры находятся в свободном обороте и без специального разрешения доступны для приобретения, например, через интернет-магазины. Однако в отдельных ситуациях существенным недостатком становится возможность визуального обнаружения данного устройства пользователем – так, под угрозой оказывается оперативно-розыскное мероприятие, направленное на получение свободных образцов компьютерного почерка.

Наконец, вибро-акустические комплексы работают по следующему принципу: они улавливают звуковую волну и вибрацию, которые возникают всякий раз при нажатии на определённые клавиши, формируют спектрограммы, которые затем расшифровываются. Работа данного способа перехвата клавиатурных записей возможна за счёт того, что, во-первых, сами по себе клавиши имеют разнообразное звучание, находятся на различном удалении от статично расположенного записывающего устройства, а во-вторых, для каждого человека характерны собственные сила нажатия и скорость набора текста, что не может не влиять на звуковое сопровождение процесса печати. Очевидно, что для достоверной записи

и точной расшифровки получаемых волн, записывающее оборудование должно быть очень чувствительным. Поэтому кейлоггеры вибро-акустического типа – это, чаще всего, очень большие системные комплексы, которые, за счёт своей непрактичности, применяются крайне редко⁷. В связи с этим, ниже, описывая потенциальную пользу от широкой интеграции рассматриваемой технологии, мы сосредоточимся только на первых двух видах.

Перехват клавиатуры позволяет определить ряд характеристик, отвечающих за индивидуальный компьютерный почерк человека⁸: степень его выработанности (в котором раскрываются число используемых пальцев, количество допускаемых ошибок и число набранных за единицу времени символов), динамика печати, темп и скорость создания текста, сила нажатия на клавиши. В свою очередь, приведённые показатели позволяют сделать выводы об исполнителе печатного текста, его физиологическом и психоэмоциональном состоянии, комфортности и привычности внешних условий, сопровождавших процесс печати.

Как было указано в начале, многие считают, что сфера применения кейлоггеров ограничивается противозаконной деятельностью,

⁶ Что такое кейлоггер? // SPY-SOFT.NET. URL: <https://spy-soft.net/chto-takoe-kejlogger-vidy-klaviaturnyx-shpionov/> (дата обращения: 09.11.2021).

⁷ Догваль В. А. Захват параметров клавиатурного почерка и его особенности // Информационные системы и технологии в

моделировании и управлении. Материалы всероссийской научно-практической конференции. Ответственных редактор Н. Н. Олейников. 2017. С. 231.

⁸ Перегудов А. В. Анализ клавиатурного почерка. Способы его применения // Interactive science. 2018. № 6 (28). С. 60.

потому что широкую огласку получает информация о том, как посредством данной технологии совершаются компьютерные мошенничества и незаконная слежка за человеком, приводящая к утечке персональных данных пользователя. Однако такое представление раскрывает кейлоггеры только с одной, негативной стороны, на самом деле их возможно применять с пользой. Наиболее полно раскрыть свой потенциал они могут в трёх сферах: трудового права, уголовного и гражданского процессов.

Для начала опишем, какое место они способны занять в отношениях между работником и работодателем. В производственной сфере кейлоггеры, позволяя определить психофизиологическое состояние работника, способствуют выявлению усталости или специфических состояния (например, алкогольного опьянения), грозящих нежелательными последствиями различной степени тяжести, вплоть до аварий⁹: так, неправильная оценка авиадиспетчером обстановки, несвоевременная реакция и ошибочная наводка, данная пилоту, могут привести к крушению самолёта. С другой стороны, отслеживая с помощью данной технологии активность пользователя, работодатель обладает действенным рычагом противодействия безделью или нецелевому использованию рабочего компьютера. Наконец, настроив аутентификацию на рабочем месте по компьютерному почерку человека,

можно избежать ситуаций выполнения определённой задачи одним сотрудником за другого и (или) предотвратить похищение друг у друга идей (в той сфере, где важна разработка индивидуальных новаторских проектов).

Безусловно, всё вышеописанное способно благоприятно сказаться на рабочих процессах, однако устанавливать кейлоггеры без уведомления работников о данном факте представляется неверным с юридической точки зрения – это может рассматриваться как несанкционированный сбор персональных данных. Поэтому в тех компаниях, где будет принято решение использовать перехватчики клавиатуры, соответствующее предупреждение следует включать в текст индивидуального и (или) коллективного трудового договора. Необходимо учитывать, что в этом случае работодатель должен дополнительно обеспокоиться защитой внутренней информационной сети с тем, чтобы избежать утечки данных о компьютерных почерках работников.

Следующими областями применения, как было указано, являются уголовный и гражданский процессы. Сейчас всё меньше текстов создаются от руки, подавляющее большинство печатаются на компьютере. Нередко возникает вопрос: кто написал тот или иной пост в блоге, кто вёл переписку через мессенджер, кто создал конкретный

⁹ Распознавание психофизиологических состояний пользователей на основе скрытого мониторинга действий в компьютерных системах / В. И. Васильев, А. Е. Сулавко, Р. В.

Борисов, С. С. Жумажанова // Искусственный интеллект и принятие решений. 2017. № 3. С. 21–23.

документ и т. п. В случае рукописных материалов для ответа на все эти вопросы назначается почерковедческая экспертиза, однако, когда в деле появляется печатный текст, она помочь не может, и каких-то других методик исследования клавиатурного почерка на настоящий момент не существует. Если же подключить в систему кейлоггеры, проблема разрешится: они позволят следователям собирать (заинтересованной стороне предоставлять) условно-свободные и экспериментальные образцы почерка для назначения по ним самостоятельной комплексной почерковедческой и компьютерно-технической экспертизы. При этом, в рамках уголовного процесса, рассматриваемая технология должна быть заимствована и оперативными сотрудниками правоохранительных органов, которые, осуществляя негласный сбор показателей посредством кейлоггеров, обеспечили бы получение свободных образцов для сравнительного исследования. На основе полученных материалов эксперты смогут устанавливать, кто напечатал текст, каким было психофизиологическое состояние исполнителя в процессе набора, какой примерный возраст исполнителя, насколько хорошо он владеет навыками печати и обращения с компьютерами в целом, а также решать другие диагностические задачи. В отдельных ситуациях от этого может зависеть ответ на вопрос о виновности

или невиновности лица (обоснованности или необоснованности заявленных исковых требований).

Однако следует указать, что внедрить систему кейлоггеров в уголовный и гражданский процессы несколько сложнее, чем в сферу трудовых отношений. В данном случае требуется обучить экспертов в сфере компьютерных технологий работе с кейлоггерами, безопасному извлечению их показателей из памяти компьютера, эксперты-почерковеды должны сформировать навыки сравнительного исследования расшифрованных отчётов, с фундаментальной стороны важно разработать научную основу, методические рекомендации для исследования компьютерного почерка и правильной интерпретации его признаков и их вариативности¹⁰. Помимо этого, большим подспорьем для следователей и определяющим условием при рассмотрении гражданско-правовых споров, где встаёт вопрос об определении личности исполнителя напечатанного текста, будет популяризация в обществе идеи обеспечения личной защиты с помощью кейлоггеров, что будет сопровождаться добровольным использованием данной технологии – это разрешит проблему получения свободных образцов почерка.

Последнее вполне возможно, поскольку кейлоггеры не обязательно передают собранные данные третьим лицам – установив себя в качестве их

¹⁰ Фёдоров И. З. К вопросу об установлении исполнителя электронного текста по клавиатурному почерку при раскрытии и

расследовании преступлений // Вестник Барнаульского юридического института МВД России. 2019. № 2 (37). С. 114.

адресата, пользователь имеет возможность применять данную технологию для решения задач личной безопасности. С одной стороны, можно дополнительно защитить свою персональную и другую личную информацию посредством настройки двойной аутентификации¹¹: система принимает пароль только в том случае, если он введён исполнителем, компьютерный почерк которого зафиксирован программой. Такое применение рассматриваемых систем позволяет эффективно противодействовать мошенникам¹². С другой стороны, установив кейлоггер на домашнем компьютере, можно контролировать контент, к которому обращаются дети, чтобы вовремя отследить потенциально опасные и (или) вредные сервисы. При этом, внедрив перехватчик клавиатуры в собственных интересах, можно дополнительно оказать значительную помощь сотрудникам правоохранительных органов и заручиться источником доказательств, если встанет вопрос определения исполнителя текста, созданного на пользовательском оборудовании.

В свете сказанного выше, кажется, что проще было бы в императивном порядке обязать всех производителей компьютеров

изначально внедрять кейлоггеры в каждую операционную систему, связывая их с защищённой единой государственной базой данных. Однако в действительности такое предложение не реализовать: это повлечёт дополнительные расходы со стороны производителей, вынудив их ещё выше поднять цены на компьютерную продукцию, спровоцирует перегрузку серверов, где собраны материалы будут храниться, и увеличит риск утечки персональных данных пользователей, таким образом а) нарушив стабильный интернет-трафик; б) создав больше возможностей совершать преступления (особенно мошеннические), чем предотвращать их. Впрочем, не имея достоверной информации, так как различные источники противоречат друг другу^{13,14}, можно всё-таки предположить, что в операционные системы внедрены программы-перехватчики, направляющие корпорациям сведения, позволяющие, например, регулярно разрабатывать новые, более удобные для пользователей клавиатуры – если это на самом деле так, то в ходе расследования преступлений можно запросить предоставление свободных образцов компьютерного почерка у

¹¹ Аверин А. И., Сидоров Д. П. Аутентификация пользователей по клавиатурному почерку // Огарёв-Online. 2015. С. 4.

¹² Как разработать систему, которая распознает человека по клавиатурному почерку // IDFinance. 2018. 27 апр. // URL: <https://habr.com/ru/company/idfinance/blog/354492/> (дата обращения: 09.11.2021).

¹³ Догваль В. А. Захват параметров клавиатурного почерка и его особенности //

Информационные системы и технологии в моделировании и управлении: Материалы всероссийской научно-практической конференции / ответ. ред. Н. Н. Олейников. 2017. С. 231.

¹⁴ Where does Windows 10 save Keyboard input? URL: <https://security.stackexchange.com/questions/143322/where-does-windows-10-save-keyboard-input> (дата обращения: 10.11.2021).

соответствующих разработчиков программного обеспечения.

В заключение хотелось бы подчеркнуть, что кейлоггеры на настоящий момент очень слабо интегрированы в нашу жизнь, а возможности широкомасштабного и реально действенного их использования напрямую зависят от сознательности граждан – ведь только на них лежит ответственность за принятие решения об установке данных систем. Однако уже сейчас производственная сфера и правоохранительная система могут начать апробацию рассмотренной

технологии, а учёным в сфере трудового права, криминалистики, уголовного и гражданского процессуального права следует обратить внимание на феномен компьютерного почерка и разработать методики его экспертного исследования и использования данных о нём в практической сфере. Это, на наш взгляд, очень важно в условиях, когда наметился тренд на полный отказ от рукописей – все сферы жизни общества должны быть готовы достойно встретить новые реалии и вызовы научно-технического прогресса.

Список литературы

1. Аверин А. И. Аутентификация пользователей по клавиатурному почерку / А. И. Аверин, Д. П. Сидоров // Огарёв-Online. 2015. С. 1–6.
2. Догваль В. А. Захват параметров клавиатурного почерка и его особенности // Информационные системы и технологии в моделировании и управлении: Материалы всероссийской научно-практической конференции / ответ. ред. Н. Н. Олейников. 2017. С. 230–236.
3. Как разработать систему, которая распознает человека по клавиатурному почерку // IDFinance. 2018. 27 апр. URL: <https://habr.com/ru/company/idfinance/blog/354492/>.
4. Клавиатурные шпионы или как клавиатура может предать вас // Новости мира IT: блог на платформе «Дзен». 2019. 11 окт. URL: https://zen.yandex.ru/media/it_news/klaviaturnye-shpiony-ili-kak-klaviatura-mojet-predat-vas-5da04457ba281e00b3fa7a4d.
5. Перегудов А. В. Анализ клавиатурного почерка. Способы его применения // Interactive science. 2018. № 6 (28). С. 59–60.
6. Распознавание психофизиологических состояний пользователей на основе скрытого мониторинга действий в компьютерных системах / В. И. Васильев, А. Е. Сулавко, Р. В. Борисов, С. С. Жумажанова // Искусственный интеллект и принятие решений. 2017. № 3. С. 21–37.
7. Фёдоров И. З. К вопросу об установлении исполнителя электронного текста по клавиатурному почерку при раскрытии и расследовании преступлений // Вестник Барнаульского юридического института МВД России. 2019. № 2 (37). С. 113–116.
8. Что такое кейлоггер? // SPY-SOFT.NET. URL: <https://spy-soft.net/chto-takoe-kejlogger-vidy-klaviaturnyx-shpionov>.

9. Design and Evaluation of a Pressure-Based Typing Biometric Authentication System / W. Eltahir, M. Salami, A. Ismail, W. Lai // EURASIP Journal on Information Security. 2008. Vol. 14. Article ID 345047.
10. Grabham N., White N. Use of a novel keypad biometric for enhanced user identity verification // Instrumentation and Measurement Technology Conference Proceedings, IMTC 2008. IEEE, 2008. P. 12–16.
11. Herley C., Florencio D. Microsoft Research How To Login From an Internet Cafe Without Worrying About Keyloggers // Symposium on Usable Privacy and Security (SOUPS). 2006. july. URL: <https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/soups06.pdf>.

Anna D. Tsvetkova

Student,

Ural State Law University named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)

Scientific supervisor – D. V. Bakhteev, PhD (Law), Associate Professor, Associate
Professor of the Department of Criminalistics

LEGAL ASPECTS OF THE USE OF KEYLOGGERS

Abstract: The paper reveals the essence of keyloggers, characterizes each of their types. Possible reasons for the negative attitude towards this technology are also considered. The following describes useful information that can be obtained with the help of keyloggers and provides models of their practical application in the field of labor relations, criminal and civil proceedings, which is accompanied by illustrating situations where the technology in question is irreplaceable. At the end, the obstacles currently existing for the widespread introduction of keyloggers are described and the necessity of overcoming them through further scientific developments on the proposed topic is substantiated.

Keywords: keylogger, computer handwriting, identification of the performer of the text, control of work processes, user authentication, control of network content.

Эмирбеков Фарид Язибекович

Студент,

Уральский государственный юридический университет

имени В. Ф. Яковлева

(г. Екатеринбург, Российская Федерация)

emirbekov.farid00@mail.ru

Научный руководитель – М. В. Гончаров, кандидат юридических наук,
доцент кафедры конституционного права

ВОЗМОЖНОСТЬ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ СЛЕДОВАТЕЛЯ

Аннотация: В статье представляется авторская позиция по поводу использования различных возможностей искусственного интеллекта в целях предупреждения, раскрытия и расследования преступлений. Приводятся аргументы о взаимосвязи эффективности применения технологии больших данных и искусственного интеллекта в этом отношении. Рассматривается мировой опыт и направления его развития, а также мнения учёных и практиков.

Ключевые слова: информационные технологии, информация, цифровизация, расследование преступлений, искусственный интеллект, большие данные.

Для цитирования:

Эмирбеков Ф. Я. Возможность использования искусственного интеллекта в профессиональной деятельности следователя // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 248–254.

Общество сравнительно давно привыкло к тому, что новейшие достижения научно-технического прогресса первой берёт на вооружение преступная среда. Не стали исключением и современные информационные технологии, которыми с момента их появления активно пользуются в своих преступных интересах криминальные элементы. Возможности таких технологий совершенствуются каждый

день, что усложняет работу правоохранительных органов по выявлению, раскрытию и расследованию преступлений, совершаемых с их использованием.

Сегодня совершенно очевидно, что повышение эффективности деятельности правоохранительных органов на данном направлении напрямую зависит от освоения ими возможностей цифровизации и их грамотного применения для целей

предупреждения, выявления и расследования преступлений. Организованная преступная деятельность стала настолько высокотехнологичной, что использование ею искусственного интеллекта и технологии больших данных уже перестало быть «проблемой завтрашнего дня», то есть возникает необходимость решать её безотлагательно, и, прежде всего, посредством внедрения соответствующих направлений в правоохранительную практику.

В целях повышения осведомлённости правоохранительных органов разных стран в июле 2018 года Интерпол совместно с Межрегиональным научно-исследовательским институтом ООН по вопросам преступности и правосудия организовали в г. Сингапур форум по вопросам искусственного интеллекта и робототехники, в июле 2019 года ими же было организовано второе Глобальное совещание в целях расширения использования данных направлений в правоохранительной деятельности. В настоящее время разработки, связанные с ИИ, ведутся в США, Германии, России, Японии и многих других развитых странах. В России 10 октября 2019 была утверждена Национальная стратегия развития искусственного интеллекта до 2030 года¹.

Информационные технологии прочно заняли своё место в нашей

жизни. «Умные» вещи, использующие технологии машинного обучения, стали повседневностью. В тесной связи с продвижением систем искусственного интеллекта развивается и программа «Умный город», технологии которого, включающие программы распознавания лиц, уже стали обыденным явлением в большинстве развитых стран. Основным источником данных для умного города являются камеры видеонаблюдения. Так, в Лондоне на 1 км² приходится свыше 300 камер наружного видеонаблюдения. В Нью-Йорке единая система сбора и анализа данных, состоит из сотен тысяч камер, аудио- и вибродатчиков и способна определить факты совершения противоправных действий и применения огнестрельного оружия. Также информация с камер поступает в центр организации дорожного движения. В Сиднее система SCATS позволяет учитывать степень загруженности дорог. Похожие программы есть в Пекине, Сингапуре и Берлине².

Автоматизация процессов управления позволяет из разрозненных информационных систем отдельных служб и ведомств создать единое информационное пространство, а технологии машинного обучения и элементы искусственного интеллекта делают город по-настоящему «умным». Инфраструктура такого

¹ Указ Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» // Официальный интернет-портал правовой информации pravo.gov. URL: <http://publication.pravo.gov.ru/Document/>

View/0001201910110003 (дата обращения: 11.05.2022).

² Воскобитова Л. А. Уголовное судопроизводство и цифровые технологии: проблемы совместимости // Lex Russica. 2019. № 5. С. 91–104.

населённого пункта предполагает, что система сбора данных позволит получать информацию о происходящем, системы хранения и обработки больших данных на основе накопленных массивов и алгоритмов машинного обучения будут выполнять анализ, а его результаты – передаваться через различные сервисы, обеспечивающие управление всеми процессами.

Обеспечение безопасности как одно из основных направлений применения камер в «умном» городе предполагает использование технологии Computer Vision (компьютерное зрение – CV), позволяющей компьютерным системам анализировать изображения и видео. Это помогает не только обнаруживать лиц и объекты, но и отслеживать их перемещения в режиме онлайн. Сегодня компьютерное зрение в видеонаблюдении и безопасности занимает 32 % от общего объёма его применения на разных направлениях. Системы интеллектуального видеонаблюдения для автоматического распознавания событий или предметов на кадрах активно используются в России уже в течение нескольких лет в области транспортной безопасности, предотвращения террористических угроз. Незаменимы такие системы и для обеспечения общественной безопасности, так как позволяет оперативно реагировать на чрезвычайные ситуации и получать дополнительные материалы для расследования преступлений. Так, в одном из пилотных проектов все крупные объекты транспортной инфраструктуры оснастили системой

распознавания лиц (четыре региональных аэропорта, два морских порта, железнодорожный вокзал). Каждый приезжающий в регион или покидающий его, оказывался в зоне действия биометрических камер. Система распознает в видеопотоке лица, строит их математические модели и сравнивает с базами розыска соответствующих ведомств. В случае совпадения, сотруднику ведомства мгновенно отправляется уведомление. За год обрабатывается до 3 миллионов лиц: пассажиры, провожающие, сотрудники транспортной инфраструктуры, которые проходят через точки контроля. Система идентифицирует 98 % лиц в потоке, что на 15 % превышает средние показатели традиционных технологий видеонаблюдения. Соответственно, биометрическая видеоидентификация позволяет найти нужные изображения с тысячами записей в базах данных различных структур и опознать человека. Сегодня можно совершенно определённо говорить о значительных возможностях компьютерного зрения для целей выявления, раскрытия и расследования преступлений.

Также, в интересах правоохранительных органов, в том числе в направлении деятельности по раскрытию и расследованию преступлений, перспективно использование возможностей CV в сфере документооборота и делопроизводства, в частности, для распознавания текста и автоматизации процесса «бумажной» работы.

Технологии компьютерного зрения сегодня бурно развиваются. Ожидается, что в недалёком будущем произойдёт повышение качества и

достоверности алгоритмов машинного зрения, расширив их возможности в области выявления и предотвращения преступлений³. При этом очевидны два тренда:

1) распространение «умных» камер, к которым применим вычислитель, способный автономно просчитывать различные сценарии видеоанализа;

2) появление услуг «облачного CV», когда все ресурсоёмкие вычисления будут выполняться на внешней (по отношению к заказчику) инфраструктуре, а заказчик лишь обеспечит трансляцию соответствия видеопотоков.

Технологии искусственного интеллекта, предполагающие в том числе и создание качественной системы сбора, хранения, обработки и анализа больших данных позволяют решать самые сложные задачи. В условиях повсеместной цифровизации деятельность правоохранительных органов невозможна без больших данных и их своевременного анализа и оценки. Практика демонстрирует острую необходимость совершенствования технических возможностей их эффективной обработки для повышения потенциальной полезности этих массивов информации.

Следует отметить, что искусственный интеллект в целом, рассматривается в двух смыслах⁴:

- как применение соответствующих технологий для решения частных задач,

- как реализация всего комплекса действий (например, по уголовному делу), то есть полноценная замена человека.

Необходимость программ автоматизированного интеллектуального анализа и прогнозирования на основе больших данных предопределяется их разноформатностью, «загрязнённостью» и неполнотой, что не позволяет человеку непосредственно осуществлять их анализ или прогноз. Соответственно, на первое место выходит не объём данных, которыми располагают правоохранительные органы, а наличие в их распоряжении интеллектуальных платформ анализа и прогнозирования на основе больших данных. А ими, согласно статистике, располагают правоохранительные органы не более 10 % из всех стран, обладающих хранилищами разнородных больших данных.

Большие данные дифференцируются в зависимости от формата, источника происхождения. К числу основных направлений, в которых правоохранительные органы имеют дело с большими данными, относятся:

1) сбор и хранение информации о ДНК;

2) сбор и хранение биометрической информации,

³ Лебедев М. Д., Саввоев С. А. Использование искусственного интеллекта в расследовании преступлений // Вопросы студенческой науки. 2020. № 7(47). С. 75.

⁴ Бахтеев Д. В. Искусственный интеллект в криминалистике: состояние и перспективы использования // Российское право: образование, практика, наука. 2018. № 2. С. 43–49.

связанной с отпечатками пальцев, радужной оболочкой глаза, а также татуировками;

3) видеонаблюдение в общественных местах.

В то же время, возможности анализа этих данных весьма ограничены. Даже, казалось бы, на наименее сложном направлении – видеонаблюдении, несмотря на наличие терабайтов видеозаписей, пока нет платформы, позволяющей осуществлять анализ по многим параметрам.

Тем не менее, наглядные примеры сравнительно эффективной работы искусственного интеллекта по обработке больших данных в правоохранительных органах ряда зарубежных стран свидетельствуют о перспективности внедрения таких возможностей. Это и система Compstat в Нью-Йорке, и программа распознавания по фрагментам татуировок, разработанная в 2014 г. ФБР совместно с Cytscadia и Cure Metrix⁵. В то же время, нельзя не учитывать и выявляемые в процессе реализации различного рода программ проблемы.

Так, в апробирование в 2013–2016 гг. в США межведомственной экспериментальной программы «Искусственный интеллект в расследовании и оперативно-розыскной деятельности при совершении уголовных преступлений» показало, что в концепции безбумажного документооборота игнорируется принцип интерактивности, лежащий в основе

формирования отчётов и документации в ходе оперативно-розыскной деятельности, при котором качественный, обеспечивающий конечный результат отчёт является плодом не индивидуальной деятельности оперативника, а результатом диалога внутри оперативной группы.

Всё больше исследователей склоняются к мнению, что к искусственному интеллекту следует относить такие программные платформы, которые позволяют эффективно решить в приемлемые сроки ту или иную задачу с использованием метода чёрного ящика, то есть недоступным для понимания человека способом в ограниченный промежуток времени. В этой связи весьма актуальны многослойные нейронные сети. В случае их использования человеку подчас непонятно, по какому алгоритму компьютер решил задачу.

Считается, что в ближайшее время такой подход будет доминировать в целом в отношении использования возможностей искусственного интеллекта. Однако перспективы его реализации правоохранительными органами неоднозначны, поскольку, даже при в целом позитивных результатах работы искусственного интеллекта, вряд ли общество в обозримом будущем сможет осудить человека на основе вердикта искусственного интеллекта.

Принципиально важно понимать, что следователь может использовать искусственный

⁵ Обзор отдельных вопросов в области больших данных и искусственного

интеллекта / под ред. В. С. Овчинского. М.: ФКУ «ГИАЦ МВД России», 2019. С. 53–54.

интеллект в своей работе для повышения её эффективности, однако последний не может подменять человека. Другими словами, следователь, располагающий инструментами ИИ, имеет несомненные преимущества перед коллегой, который их не использует. В настоящее время внедрение ИИ в деятельность следственных подразделений находится в зачаточном состоянии.

Предстоит большой по объёму и сложности путь, однако, это отнюдь не означает, что он будет долгим, поскольку скорость развития всех информационных процессов в обществе и на разных направлениях внедрения современных, в том числе цифровых, технологий, колоссальна – она не просто в разы, а в десятки и сотни раз быстрее предыдущих этапов развития НТП. Тем не менее, пока ясно одно: предстоит провести немало научных исследований и практических испытаний, чтобы стало возможным и доступным массовое и повсеместное применение искусственного интеллекта в деятельности следственных подразделений⁶.

Использование искусственного интеллекта следователем предполагает обоснованную постановку задач, унифицированный алгоритм обучения и последующего тестирования, апробации на практике. В целом, процесс внедрения ИИ в деятельность следственных подразделений должен включать такие стадии как:

1) научная разработка и обоснование;

2) создание алгоритма применения:

- условия включения в работу,
- минимальный объём исходных данных,
- описание действий по их оценке,
- описание вариантов принимаемых решений и их аргументации;

3) тестовые испытания;

4) применение с постоянным мониторингом «побочных» эффектов.

Действительно, ИИ позволяет правоохранительным органам добиваться серьёзных успехов в борьбе с организованной преступностью, тем не менее, даже при высоком качестве материально-технической базы и программно-аппаратного обеспечения, их потенциал не реализуется из-за низкого уровня компьютерной грамотности служащих, во многих случаях заметно уступающего уровню преступников.

Таким образом, перспектива замены искусственным интеллектом следователя, как и любого другого участника уголовного судопроизводства, уполномоченного принимать процессуальные решения, весьма далека от реальности; действительную практическую ценность несут теоретические и практические разработки, направленные на инструментальное обеспечение работы органов государственной власти в сфере уголовного судопроизводства, освобождение их от рутинной, так

⁶ Сибилькова А. В. Искусственный интеллект на службе у следователя // Российский следователь. 2019. № 3. С. 68–70.

называемой технической работы, выполнения сложных операций по исследованию физического мира, таких как моделирование событий, вещественной обстановки, образа преступника, поиск и обработка информации, формирование не

требующих сложной мотивировочной части документов, фиксирование и анализ психофизиологических реакций участников уголовного судопроизводства, обеспечение оперативной коммуникации

Список литературы

1. Бахтеев Д. В. Искусственный интеллект в криминалистике: состояние и перспективы использования // Российское право: образование, практика, наука. 2018. № 2. С. 43–49.
2. Воскобитова Л. А. Уголовное судопроизводство и цифровые технологии: проблемы совместимости // Lex Russica. 2019. № 5. С. 91–104.
3. Лебедев М. Д. Использование искусственного интеллекта в расследовании преступлений / М. Д. Лебедев, С. А. Саввоев // Вопросы студенческой науки. 2020. № 7(47). С. 75.
4. Сибилькова А. В. Искусственный интеллект на службе у следователя // Российский следователь. 2019. № 3. С. 68–70.

Farid Ya. Emirbekov

Student,

Ural State Law University
named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
emirbekov.farid00@mail.ru

Scientific supervisor – M. V. Goncharov, PhD (Law),
Associate Professor of the Department of Constitutional Law

THE POSSIBILITY OF USING ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN THE PROFESSIONAL ACTIVITY OF THE INVESTIGATOR

Abstract: The article presents the author's position on the use of various possibilities of artificial intelligence for the prevention, detection and investigation of crimes. Arguments about the relationship between the effectiveness of the use of big data technology and artificial intelligence in this regard are given. The world experience and directions of its development, as well as the opinions of scientists and practitioners are considered.

Keywords: information technology, information, digitalization, crime investigation, artificial intelligence, big data.

Раздел II

БИОТЕХНОЛОГИИ

Репродуктивные технологии

Геномные и медицинские технологии

УДК 343.9

Рачева Нелли Витальевна

Кандидат юридических наук, доцент кафедры криминалистики,
Уральский государственный юридический университет имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
e-mail: ekaterinburg@mail.ru

Костин Никита Олегович

Студент,
Уральский государственный юридический университет имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
nikit0s_2302@mail.ru

ДНК-ФЕНОТИПИРОВАНИЕ И КРИМИНАЛИСТИКА: ПЕРСПЕКТИВЫ СОТРУДНИЧЕСТВА

Аннотация: Мировые достижения в генной инженерии и компьютерных технологиях, в том числе и использование глубоких нейронных сетей, открывают новые горизонты человеческой жизни. Прогресс в этих областях позволяет облегчить мировому сообществу решение бытовых проблем, в том числе обеспечивая безопасность населения. Так, в относительно недалеком будущем уже возможно представить ситуацию, когда по одной частичке биологического материала, оставленного на месте происшествия, эксперт, прибегнув к ДНК-фенотипированию, не выходя из лаборатории, сможет составить фоторобот скрывшегося преступника.

Ключевые слова: ДНК-фенотипирование, криминалистика, ДНК-дактилоскопия, нераскрытые преступления, генетические технологии.

Для цитирования:

Рачева Н. В., Костин Н. О. ДНК-фенотипирование и криминалистика: перспективы сотрудничества // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 256–265.

Ежегодно, согласно статистике Генеральной прокуратуры Российской Федерации, в России наблюдается значительный процент нераскрытых преступлений. Так, в 2021 г. таковых

насчитывалось 58 %, из них тяжких и особо тяжких – около 31,6 %¹. Об этой проблеме заявлял в 2020 г. и Генеральный прокурор России

¹ Динамика показателей преступности // Портал правовой статистики Генеральной прокуратуры Российской Федерации. URL:

http://crimestat.ru/offenses_chart (дата обращения: 10.05.2022).

И. В. Краснов², констатируя, что «общий уровень раскрываемости за 2020 г. снизился до 52 %. Остались нераскрытыми 963 тыс. криминальных деяний». При этом, как отмечает И. В. Краснов, совершается всё больше преступлений против половой неприкосновенности несовершеннолетних. За последние 10 лет количество подростков и детей, пострадавших от таких деяний, выросло на 63 %. Как следует из статистики, довольно большой объём нераскрытых преступлений как раз относится к посягательствам на жизнь и здоровье, а также на половую свободу и неприкосновенность личности.

К сожалению, чем больше времени проходит с момента совершения таких преступлений, тем сложнее раскрыть уголовное дело – в этом случае время «работает» против правоохранительных органов. Однако нивелировать эту проблему помогают современные технологии и научные прорывы в самых разнообразных областях: начиная компьютерными и цифровыми системами и заканчивая геномными исследованиями. Так, если с ростом кибер-преступности всё большее внимание уделяется достижениям в области ИТ-технологий, то в расследовании традиционных преступлений огромный вклад вносят достижения генной инженерии и последующее внедрение их в правоприменительную деятельность. На этом фоне всё чаще криминалистов

интересуют новейшие технологии в генетике, позволяющие не только успешно расследовать «свежие» преступления, но и раскрывать дела, которые в силу объективных и субъективных факторов не были расследованы. Таким образом, популярность приобретают методы установления личности преступника путём сравнения его биологического материала, обнаруженного на месте происшествия, с образцами, изъятыми у подозреваемого, а также возможность проектирования по оставленным биоматериалам предположительных характеристик преступника. Именно эта область ДНК-дактилоскопии под названием ДНК-фенотипирование и является на сегодняшний день одной из самой перспективных и многообещающих сфер в развитии криминалистических исследований.

Необходимо отметить, что мировые технологические успехи в сфере изучения геномов, ворвавшиеся в человеческую жизнь в конце прошлого века, изменили мир так сильно, что без них нашу действительность невозможно представить. Не обошло это «новшество» и криминалистику, где уже многие годы генетическая идентификация используется как относительно быстрый метод, который позволяет посредством соответствующей базы данных категорично ответить на вопрос принадлежности конкретному

² Генеральный прокурор Российской Федерации Игорь Краснов выступил с докладом в Совете Федерации // Генеральная прокуратура Российской Федерации:

официальный сайт. URL: <https://epp.genproc.gov.ru/web/gprf/mass-media/news?item=61267146> (дата обращения: 10.05.2022).

человеку крови, волос, спермы, обнаруженных на вещественных доказательствах.

Генетика зародилась более ста пятидесяти лет назад, когда в 1869 г. швейцарский врач и биолог Иоганн Фридрих Мишер открыл нуклеиновые кислоты³, представление о которых со временем перевернуло человеческий мир. К середине XX века стало понятно, что ДНК и РНК являются носителями наследственной информации, затем была описана их структура, а чуть позднее – появились многочисленные методы, позволяющие, к примеру, «нарезать» эти молекулы в пробирке с помощью клеточных ферментов рестриктаз; амплифицировать их, используя метод ПЦР и, что оказалось более применимо в раскрытии преступлений – читать последовательности конкретных генов и геномов, применяя при этом многочисленные методы секвенирования⁴. В этой связи новыми возможностями анализа генетического материала заинтересовались и криминалисты всего мира. Произошло это вследствие того, что традиционные и привычные к тому времени методы классической дактилоскопии и анализа групп крови имели свои ограничения, и в некоторых случаях приводили к серьёзным ошибкам. Наиболее ярким

примером этого является уголовное дело А. В. Чикатило, когда в ходе предварительного расследования была проведена судебно-биологическая экспертиза крови подозреваемого определившая вторую (В) группу, однако, как оказалось впоследствии – ошибочно. Ценой этого, по словам известного криминалиста Иссы Костоева, стали человеческие жизни⁵.

Начало для использования новейших генетических технологий в криминалистике было положено в 1984 году, когда британский учёный Алек Джеффрис разработал и представил метод идентификации личности человека с использованием его генетического материала. В дальнейшем это получило название ДНК-дактилоскопии (или ДНК-идентификации), заслужив признание и уважение у криминалистов всего мира, а Джеффрис стал пионером геномных исследований в правоприменительной сфере. Анализ ДНК в судебном следствии по сей день предоставляет доказательственный материал такой точности, которую не способны дать иные инструменты криминалистики⁶.

Отечественные учёные и исследователи также не отставали от зарубежных коллег и сделали множество открытий в этой сфере. К

³ Мамедова С. М. К 50-летию открытия структуры ДНК // Биомедицина (Баку). 2003. № 1. С. 36–41.

⁴ Недолужко А. Криминалистика. Молекулярно-генетическая экспертиза // Биомолекула. 2020. URL: <https://biomolecula.ru/articles/kriminalistika-molekuliarno-geneticheskaia-ekspertiza> (дата обращения: 08.05.2022).

⁵ Исса Костоев: «При анализе крови Чикатило произошла ошибка. Ценой которой стали

человеческие жизни» // Пражский Телеграф. 2015. № 23/316. URL: <https://ptel.cz/2015/06/issa-kostoev-pri-analize-krovi-chikatilo-proizoshla-oshibka-cennoj-kotoroj-stali-chelovecheskie-zhizni/> (дата обращения: 09.05.2022).

⁶ Генетика – судебной экспертизе Беларуси / А. Кильчевский, И. Моссэ, М. Шаптуренко, А. Буракова // Минск: Наука и инновации. 2020. № 10 (212). С. 22–28.

примеру, рассматривая начальные этапы ДНК-идентификации личности в Российской Федерации, необходимо обратить внимание на труды член-корреспондента РАН А. П. Рыскова, под руководством которого в СССР были начаты исследования по геномной дактилоскопии и обнаружено особое семейство универсальных гипервариабельных повторов ДНК в геномах человека, животных, растений и микроорганизмов. В 1996 г. за разработку теоретических и прикладных проблем геномной дактилоскопии А. П. Рысков вместе с коллективом соавторов (Г. П. Георгиев, С. А. Лимборская, М. И. Просняк, П. Л. Иванов, Е. И. Рогаев, А. Г. Джинчарадзе) стали Лауреатами Государственной премии Российской Федерации⁷.

В отечественной криминалистике методы ДНК-анализа получили название генотипоскопии и их использование началось в 1988 г., когда Государственным комитетом СССР по науке и технике было принято решение об организации лаборатории генотипоскопии на базе Всесоюзного научно-криминалистического центра МВД СССР (ныне Экспертно-криминалистический центр МВД России), а первая генотипоскопическая экспертиза этой структурой была проведена в 1990 году⁸. В 1994 г. было принято решение утвердить

«Федеральную программу Российской Федерации по усилению борьбы с преступностью на 1994–1995 годы», где говорилось о создании на базе имеющихся экспертных учреждений единой системы генно-дактилоскопических учётов, но из-за экономических трудностей работа в этом направлении была тогда приостановлена.

На рубеже веков на коллегии МВД России от 15.01.99 г. № 1 вновь прозвучал вопрос о необходимости создания соответствующей базы данных ДНК для поиска в ней лиц, являющихся возможным источником происхождения изъятых биологических объектов при отсутствии сравнительных образцов, путём сопоставления генетических признаков исследуемого объекта и хранящейся в базе данных информации о ДНК подучётных лиц⁹. При этом фактически первая база данных ДНК в России была создана лишь в 2006 году в рамках экспертно-криминалистического учёта данных ДНК биологических объектов, утверждённого и регламентированного Приказом МВД от 10.02.2006 № 70 «Об организации использования экспертно-криминалистических учётов органов внутренних дел Российской Федерации».

В настоящее время в России действует Федеральный закон от 03.12.2008 г. № 242-ФЗ «О государственной геномной

⁷ Рысков А. П. Хроника // Генетика. 2011 Т. 47 (2). С. 284–285.

⁸ Пименов М. Г., Культин А. Ю., Кондрашов С. А. Научные и практические аспекты криминалистического ДНК-анализа. М.: ГУ ЭКЦ МВД России, 2001. 144 с.

⁹ ДНК-криминалистика — зарождение, современность и перспективы / В. А. Анисимов, Р. Р. Гарафудинов, А. М. Сагитов [и др.] // Биомика. 2019. Т. 11 (3). С. 282–314.

регистрации в Российской Федерации», который послужил правовой основой для создания федеральной базы данных геномной информации Российской Федерации. Так, согласно ст. 7 данного Федерального закона, обязательной государственной геномной регистрации подлежат:

1. лица, осуждённые и отбывающие наказание в виде лишения свободы за совершение тяжких или особо тяжких преступлений, а также всех категорий преступлений против половой неприкосновенности и половой свободы личности;

2. неустановленные лица, биологический материал которых изъят в ходе производства следственных действий;

3. неопознанные трупы.

Вклад базы данных ДНК в раскрытие преступлений невозможно переоценить: так, согласно статистике, сообщённой пресс-центром МВД России, с 2009 по 2021 года более 30 тыс. преступлений, в основном тяжких и особо тяжких, удалось раскрыть с помощью использования ресурсов федеральной базы данных геномной информации, установив при этом более 70 тыс. лиц, которые были причастны к совершению преступлений¹⁰. Таким образом, использование геномной информации в расследовании преступлений является

эффективным средством, приносящим впечатляющие результаты. Однако для ещё большей эффективности использования генетической базы данных, можно обратить внимание на неоднократные предложения председателя Следственного Комитета Российской Федерации А. И. Бастрыкина: произвести обязательную геномную регистрацию всех трудовых мигрантов из стран ближнего зарубежья¹¹. Предполагается, что данные меры будут носить превентивный характер, позволяя установить личность преступника, не являющегося гражданином Российской Федерации и оставившего биологические следы на месте происшествия.

Всё вышесказанное является правовой основой для развития геномных технологий, позволяющих раскрывать неочевидные преступления, в нашей стране. Однако не стоит ограничиваться лишь рамками собственных научных изысканий, необходимо также обращать внимание и внедрять в практическую деятельность положительный опыт других странах. Так, развитие геномики, физической антропологии, методов магнитно-резонансной и компьютерной томографии, 3D-моделирования, а также нейросетевых алгоритмов сделали возможным восстановление облика человека по его биологическому материалу. Эту

¹⁰ В МВД назвали число раскрытых благодаря базе данных ДНК преступлений // РБК. 2021. 8 мая. URL: <https://www.rbc.ru/rbcfreenews/6096007d9a794728f4031a2d> (дата обращения: 10.05.2022).

¹¹ Козлова Н. Бастрыкин выступил за обязательную геномную регистрацию

трудовых мигрантов // Интернет-портал «Российской газеты». 2021. 1 ноя. URL: <https://rg.ru/2021/11/01/bastrykin-vystupil-za-obiazatelnuiu-genomnuiu-registraciiu-trudovyh-migrantov.html> (дата обращения: 05.05.2022).

молодую область ДНК-дактилоскопии называют ДНК-фенотипированием, она начала развиваться лишь в начале XXI века и быстро продвигается вперёд. Так, в 2012 году в Северной Каролине, составленный на основе ДНК-фенотипирования портрет предполагаемого преступника, указал на одного из подозреваемых в двойном убийстве. В 2017 г. Публикация в Техасе ДНК-фоторобота подозреваемого в убийстве позволила задержать человека, которого прежде полиция вообще никак не связывала с совершением преступного посягательства. Таким образом, это новейшая система разнообразных технологий (от генетических до IT-технологий) уже в начале своего применения даёт существенные результаты в раскрываемости преступлений, в том числе прошлых лет.

Среди основоположников фенотипирования выделяют криминалистов Манфреда Кайзера и Сьюзан Уолш, которые создали метод IrisPlex для определения цвета глаз по нескольким маркерам в ДНК. Впоследствии он был расширен некоторыми дополнительными генами для выяснения цвета волос и кожи. После многочисленных этапов обучения нейронная сеть стала определять не только этническую принадлежность или морфологические признаки (цвет глаз или волос), но и воссоздавать облик человека по образцу ДНК, полученному с места происшествия.

Сегодня обучение глубоких нейронных сетей является наиболее развивающимся направлением в областях машинного обучения и

искусственного интеллекта. Наблюдается бурный рост методов применения глубоких нейронных сетей как в создании фотореалистичных изображений, так и в геномных исследованиях, что является крайне актуальным для криминалистики. К примеру, прогнозирование внешнего облика (фенотипа) человека с помощью его генетической информации активно развивается и уже успешно применяется правоохранительными органами Соединенных Штатов Америки. Нью-Йорк – первый город в США, где полиция использует ДНК-фенотипирование для раскрытия неочевидных преступлений. Правда, говорить о широкой практике рано – к концу 2017 года новую технологию освоила всего лишь одна городская лаборатория. Однако в настоящее время количество лабораторий постоянно возрастает. Это позволяет извлекать из архивов приостановленные дела и раскрывать их благодаря генетической информации и современным компьютерным технологиям. Одной из компаний, предоставляющих услуги по фенотипированию ДНК для правоохранительных организаций, является Parabon NanoLabs, разрабатывавшая данную технологию и базирующаяся в Рестоне, штат Вирджиния. По словам Эллен Грейтак, одного из директоров Parabon NanoLabs: «этот метод позволяет не только определить пол человека, но и выявить ряд других важных деталей – составить портрет (приблизительный) со множеством подробностей, включая цвет кожи, глаз, волос, а также веснушки и родимые пятна».

В 2014 году, используя глубокий анализ данных и передовые алгоритмы машинного обучения в рамках специализированного биоинформатического конвейера, Parabon NanoLabs – при финансовой поддержке Министерства обороны США (DoD) – разработала мультиплексную систему Snapshot Forensic DNA Phenotyping System, которой ныне пользуется уже более 40 правоохранительных организаций в Америке и за её пределами. Эта система точно предсказывает генетическое происхождение, цвет глаз, цвет волос, цвет кожи, наличие веснушек и форму лица у лиц любого этнического происхождения, в том числе и смешанного. Так, SNaPshot помогла раскрыть ранее упомянутое преступление в Северной Каролине. Согласно фактическим обстоятельствам дела, преступник, застреливший в 2012 году двух человек (родителей некой Уитли), оставил на месте преступления пять капель крови. ДНК убийцы в базах данных не оказалось. Через три года полиция обратилась за помощью в Parabon. Специалисты компании установили, что преступник – латиноамериканец со светлой кожей и тёмными волосами. Используя эти данные, следователи более внимательно изучили семью мужа Уитли и вышли на его брата. ДНК подозреваемого полностью соответствовала генетическому следу, найденному в пятнах крови. Мужчину арестовали в июне 2015 года.

Преступник признал вину и получил два пожизненных срока заключения.

Snapshot использовался правоохранительными органами по всему миру, чтобы помочь найти следы, сузить круг подозреваемых и раскрыть уголовные дела прошлых лет. На сайте Parabon NanoLabs в открытом доступе находится подборка уголовных дел, раскрытых с помощью этой компании¹². Помимо Parabon NanoLabs в мире существует еще несколько организаций и компьютерных программ, позволяющих при помощи генетического материала нейросетевым алгоритмам восстанавливать облик человека по его биологическому материалу. Так, в 2017 году стартап генетика Крейга Вентера Human Longevity представил систему, обученную на полных генетических данных и результатах тщательной оценки внешности больше, чем тысячи добровольцев – только форма лица измерялась по 30 тыс. точек. По заявлению авторов, их искусственный интеллект способен делать выводы о характеристиках внешности, возрасте, весе, росте, телосложении, цвете глаз, кожи и даже голосе, причём с впечатляющей результативностью: из 20 случайных фотографий система верно выбирает обладателя определённой ДНК с вероятностью 74 %. «Из единственного отпечатка пальца мы можем секвенировать геном и определить ваш облик», – заявил по этому поводу Крейг Вентер¹³.

¹² The Snapshot DNA Phenotyping Service // Parabon NanoLabs, Inc. URL: <https://snapshot.parabon->

nanolabs.com/phenotyping (дата обращения: 07.05.2022).

¹³ Фишман Р. Портрет генами // TechInsider. 2018. 1 окт. URL:

Однако, у программы Вентера нашлось немало противников. Учёные заметили, что если предъявленный набор в программе будет содержать только людей одного пола и цвета кожи (белых мужчин), то точность идентификации падает многократно. И это притом, что именно они составили ядро использованной при обучении выборки, и именно с лицами белых мужчин искусственный интеллект работает эффективнее всего. На них же приходится и большая часть информации, накопленной в генетических и медицинских базах данных, поэтому пока результаты ДНК-фенотипирования людей других этносов куда хуже. Всё же, генетика формирования фенотипа крайне запутанна, и у представителей разных народов в создании одного признака может участвовать разный набор аллелей.

Существуют и более универсальные проблемы применения ДНК-фенотипирования. Несмотря на тот факт, что для такого исследования необходимо очень небольшое количество биологического материала, всё же существует значительный риск «загрязнения» образцов при сборе на месте происшествия, что может повлечь в дальнейшем различные ошибки. Необходимо обратить внимание и на высокую стоимость процедуры – на 2017 год это было около 4000 долларов США, сейчас цена значительно снизилась, однако постоянное использование указанных

геномных технологий всё же влечёт колоссальные затраты. К тому же, перспективы разработки криминалистического ДНК-фенотипирования зависят от решения не только научных, но и правовых вопросов.

Исследования в данной области, особенно те, которые связаны с прогнозированием поведения, здоровья, затрагивают крайне уязвимые для личности сферы, представляя тем самым потенциальную опасность для гражданских прав и свобод. К примеру, генетические заболевания и их предрасположенность исключены из судебного фенотипирования ДНК, поскольку считается, что их использование в значительной степени нарушат конфиденциальность искомых лиц¹⁴. Генетическая информация является безусловно особым объектом охраны в Российской Федерации, а значит и применение любых ДНК-технологий необходимо строго регулировать, создавая предварительно правовую основу как научных изысканий в этой области, так и практического применения их результатов.

Учитывая вышеизложенное, можно сказать, что ДНК-фенотипирование является будущим криминалистики. Рано или поздно будут идентифицированы и другие гены, определяющие внешность. Если с цветом глаз больших сложностей нет – его обуславливает не так много

<https://www.techinsider.ru/science/441622-portret-genami/> (дата обращения: 11.05.2022).

¹⁴ Краева Я. В., Рожкова В. Р. ДНК-фенотипирование: проблемы и перспективы

// Вопросы российской юстиции. 2021. № 11. С. 440–444.

аллелей, – то многие признаки полигенны. Максимально точная на сегодняшний день система определения оттенка волос по ДНК, разработанная в Королевском колледже Лондона, даёт правильные предсказания в девяти случаях из десяти и при этом использует больше 120 генетических маркеров. Не стоит забывать и о влиянии эпигенетической настройки: она не меняет последовательность ДНК, но может сказываться на результатах её работы. Поэтому секвенировать ДНК и определить коррелирующие с тем или иным признаком гены – это даже не полдела, а только самое начало. Проще всего предсказать пол носителя ДНК. Определить цвет глаз и волос сложнее, но, как правило, проблем не возникает, а другие данные, например рост, выявить однозначно пока невозможно. Ряд маркеров могут использоваться, чтобы определить биогеографическое происхождение человека. Сегодня можно достоверно определить принадлежность к основным континентальным группам – Африканской, Западно-Евразийской, Восточно- и Южно-Азиатской или Коренной Американской. Определить происхождение вплоть до страны, в

данное время, невозможно, однако, ориентируясь на динамичные и быстро развивающиеся генетические технологии, можно с уверенностью сказать, что для этого необходимо всего лишь время.

На современном этапе ДНК-фенотипирование можно назвать исследованием, которое позволит правоохранительным органам сузить круг подозреваемых, определить наиболее подходящие под описанные в исследовании характеристики личности, а затем, проведя ДНК-дактилоскопическую экспертизу, конкретизировать преступника. К тому же, ориентируясь на классификацию методов криминалистики, которую выделил известный учёный-криминалист Л. Я. Драпкин¹⁵, на наш взгляд, ДНК-фенотипирование необходимо включить в специальные методы, которые основаны на достижениях других наук (биология, IT-технологии, медицина).

Таким образом, для успешного функционирования геномных исследований в Российской Федерации существуют все предпосылки, которые необходимо развивать, в том числе используя мировой опыт в этой сфере.

Список литературы

1. Генетика – судебной экспертизе Беларуси / А. Кильчевский, И. Моссэ, М. Шаптуренко, А. Буракова // Минск: Наука и инновации. 2020. № 10 (212). С. 22–28.
2. ДНК-криминалистика – зарождение, современность и перспективы / В. А. Анисимов, Р. Р. Гарафутдинов, А. М. Сагитов [и др.] // Биомика. 2019. Т. 11 (3). С. 282–314.

¹⁵ Криминалистика в 3 ч. Часть 1: учебник для вузов / ответ. ред. Л. Я. Драпкин. 2-е изд.,

испр. и доп. Москва: Издательство Юрайт, 2018. С. 30.

3. Краева Я. В. ДНК-фенотипирование: проблемы и перспективы / Я. В. Краева, В. Р. Рожкова // Вопросы российской юстиции. 2021. № 11. С. 440–444.
4. Криминалистика в 3 ч. Часть 1: учебник для вузов / ответственный редактор Л. Я. Драпкин. 2-е изд., испр. и доп. Москва: Издательство Юрайт, 2018. 246 с.
5. Мамедова С. М. К 50-летию открытия структуры ДНК // Биомедицина (Баку). 2003. № 1. С. 36–41.
6. Недолужко А. Криминалистика. Молекулярно-генетическая экспертиза. // Биомолекула. 2020. URL: <https://biomolecula.ru/articles/kriminalistika-molekuliarno-geneticheskaja-ekspertiza>.
7. Пименов М. Г. Научные и практические аспекты криминалистического ДНК-анализа / М. Г. Пименов, А. Ю. Культин, С. А. Кондрашов. М.: ГУ ЭКЦ МВД России, 2001. 144 с.
8. Рысков А. П. Хроника // Генетика. 2011. Т. 47 (2). С. 284–285.

Nelly V. Racheva

PhD (Law), Associate Professor of the Department of Criminalistics,
Ural State Law University named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
ekaterinburgg@mail.ru

Nikita O. Kostin

Student,
Ural State Law University named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
nikit0s_2302@mail.ru

**DNA PHENOTYPING AND CRIMINALISTICS:
PROSPECTS FOR COOPERATION**

Abstract: World achievements in genetic engineering and computer technologies, including the use of deep neural networks, open up new horizons in human life. Progress in these areas makes it possible to alleviate everyday problems for the world community, including ensuring the safety of the world's population. So, in the relatively near future, it is already possible to imagine a situation when, according to one piece of biological material left at the scene, an expert, resorting to DNA phenotyping, without leaving the laboratory, will be able to make a sketch of a fugitive criminal.

Keywords: DNA phenotyping, forensics, DNA fingerprinting, unsolved crimes, genetic technologies.

УДК 340.65

Рачева Нелли Витальевна

Кандидат юридических наук, доцент кафедры криминалистики,
Уральский государственный юридический университет
имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
e-mail: ekaterinburg@mail.ru

Слепухина Яна Михайловна

Студент,
Уральский государственный юридический университет
имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
e-mail: yana_slepukhina11@mail.ru

ВИРТУАЛЬНОЕ ВСКРЫТИЕ: ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация: Статья посвящена использованию метода виртуального вскрытия трупов. Проводится параллель между развитием виртопсии в России с практикой применения в зарубежных странах, рассматривается опыт и достижения в этой сфере. Анализируются положительные и отрицательные моменты использования данного метода, а также перспективы применения в Российской Федерации.

Ключевые слова: убийство, труп, вскрытие, судебно-медицинская экспертиза, виртуальное вскрытие, компьютерная томография, магнитно-резонансная томография.

Для цитирования:

Рачева Н. В., Слепухина Я. М. Виртуальное вскрытие: перспективы применения метода в Российской Федерации // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 266–273.

Посмертная визуализация является самой молодой и перспективной областью лучевой диагностики. Первые попытки рентгенографии трупов были предприняты в 1895 г., сразу после открытия В. К. Рентгеном X-лучей. К сожалению, в то время это не вызвало

широкий интерес, так как получаемые изображения существенно отличались от современных, поскольку снимки получались в плохом качестве и были трудные для восприятия.

Реальное внедрение лучевой диагностики началось только в XX–XXI веках. Первое публичное

предложение использовать исследования компьютерным томографом (далее – КТ) в качестве альтернативы реальному вскрытию озвучено в 1994 г. В 2000 г. в Швейцарии был запущен проект, в рамках которого стали проводиться сравнительные исследования виртуального и реального вскрытия¹.

Огромные достижения в виртуальном вскрытии сделали профессора Ричард Дирнхофер и Майкл Тали. В конце девяностых они занимались реконструкциями сцен убийства, а потом одни из первых перенесли работу в виртуальное пространство. Известность пришла после расследования громкого дела в Цюрихе, где криминалисты доказали путём 3D-технологий, что орудием убийства был не гаечный ключ, оставивший на черепе жертвы две необычные раны, а иной предмет². Профессор Дирнхофер создал неологизм для идентификации проекта и процесса малоинвазивной визуальной виртуальной аутопсии, объединив слова «виртуальный» и «вскрытие» в удобное, но ёмкое слово – *virtopsy*.

Виртопсия включает с себя методику посмертного исследования тела, объединяющую проведение классического вскрытия с

предварительным использованием трёхмерного компьютерного исследования всего тела^{3,4}.

По уголовным делам об убийствах в первую очередь назначается судебно-медицинская экспертиза трупа. Она состоит из наружного и внутреннего исследований. Первое заключается в осмотре одежды и самого трупа, описании трупных изменений и других особенностей. Внутреннее исследование включает в себя вскрытие трёх основных полостей: черепа, груди и живота. Исследование производится с целью выяснения причины смерти и времени её наступления, характера имеющихся изменений, повреждений, и других вопросов, перечень которых зависит от обстоятельств расследуемого преступления и условий реальной ситуации.

Однако в некоторых случаях вскрытие затрудняется вследствие обстановки, в которой находилось тело до момента его обнаружения, например, в воде, на месте пожара и др. Трудности с установлением произошедшего и событий, предшествовавших ему, а также идентификацией личности погибшего, в основном, связаны с недостаточным или полным отсутствием

¹ *Virtopsy, a new imaging horizon in forensic pathology: virtual autopsy by postmortem multislice computed tomography (MSCT) and magnetic resonance imaging (MRI) a feasibility study / M. J. Thali, K. Yen, W. Schweizer [et al.] // Journal of Forensic Science. 2003. Vol. 48. P. 386–403.*

² *Thali M., Dirnhofer R., Vock P. The Virtopsy Approach. 3D optical and radiological scanning*

and reconstruction in forensic medicine // Boca Raton, FL: CRC Press; London NW. 2009.

³ *Virtopsy: minimally invasive, imaging guided virtual autopsy / R. Dirnhofer, C. Jackowski, P. Vock [et al.] // Radio Graphics. 2006. Vol. 26. P. 1305–1333.*

⁴ *Virtopsy – the Swiss virtual autopsy approach / M. J. Thali, C. Jackowski, L. Oesterhelweg [et al.] // Leg Med (Tokyo). 2007. Vol. 9. P. 100–104.*

вещественных доказательств на месте обнаружения трупа, быстрыми посмертными изменениями тела и т. д.⁵

Самыми распространёнными методами вскрытия считаются:

- метод комбинированного секционного разреза мягких тканей передней поверхности тела⁶,
- метод воротникового разреза с последующим вскрытием диафрагмы (разрез Лешке),
- метод комплексного извлечения органов головы, шеи, грудной, брюшной и тазовой полостей (метод Г.В. Шора).

Однако научно-технический прогресс позволил внедрить современные технологии в области диагностики тела.

Чтобы ускорить процесс вскрытия и облегчить исследование, стали использовать виртуальное вскрытие. С традиционным у него только одно сходство, заключающееся в том, что специалист, осматривающий труп, сможет увидеть всё, происходящее внутри тела. Существенное же отличие – отсутствие необходимости резать тело, так как экспертиза проводится с помощью 3D-сканирования, фотограмметрии. Фотограмметрия – это реконструкция объектов по изображениям. Раньше она использовалась для воссоздания сцен убийства или крупных сооружений по картинке, а теперь

перенесена на микроуровень, где помогает засечь самые незаметные травмы. Специальный проектор наносит трёхмерный интерференционный рисунок на поверхность тела. После этого труп помещают в сканер для компьютерной томографии и при помощи рентгеновского излучения получают «нарезку» из нескольких тысяч проекций от головы до кончиков пальцев. Метки на поверхности кожи в специальных местах помогают соотнести поверхность тела и трёхмерные сканы внутренних органов и костей, а магнитно-резонансная томография позволяет получить больше информации о мягких тканях.

Специалисты отмечают преимущество виртопсии, заключающееся в подробной наглядной иллюстрации выводов эксперта. Каждое повреждение можно рассмотреть с помощью приближения или уменьшения картинки, с разных ракурсов. Это облегчает работу сотрудникам правоохранительных органов, адвокатам и судьям⁷, так как облегчает понимание результатов работы эксперта лицами, не имеющими медицинского образования.

В судебно-медицинской практике иностранных государств данный метод активно используется уже много лет. Результаты

⁵ Новые диагностические признаки утопления по результатам виртуальной аутопсии / В. А. Клевно, Ю. В. Чумакова, М. А. Кислов [и др.] // Судебная медицина. 2020. Т. 6. № 3. С. 53–57.

⁶ Абрикосов А. И. Техника патологоанатомических вскрытий трупов. М.: Медицина, 1948. С. 54.

⁷ Дадабаев В. К., Стрелков А. А. Законодательная основа производства судебно-медицинской экспертизы и возможности применения рентгеновского метода компьютерной томографии (СКТ) в исследовании трупа // Библиотека криминалиста. 2014. № 6. С. 275–280.

виртуальной аутопсии признают суды Швейцарии, используют австралийские криминалисты, в американской армии с 2004 года на рентген и КТ отправляется тело каждого погибшего военнослужащего.

Стоит сказать, что в некоторых странах данный метод стал настолько распространённым, что является коммерческой услугой, которая доступна для всех желающих. В США можно заказать собственную посмертную виртопсию, которая поможет избежать возможных споров о наследстве: определив причину смерти человека, сам он умер или в результате убийства, можно будет исключить вероятность завладения наследством родственниками незаконным путём. Таким образом, виртопсия выступает некой гарантией того, что никто из наследников не посягнёт на жизнь заказчика.

В Швейцарии технологии зашли ещё дальше: в лаборатории Virtopsy Бернского университета уже разработали робота-патологоанатома⁸.

В экспертных учреждениях зарубежных стран, активно использующих виртопсию, есть всё необходимое оборудование. В свою очередь, в Российской Федерации только в Бюро судебно-медицинской экспертизы Московской области с июля 2018 года проводится ряд посмертных компьютерных томографий. Внимания заслуживает случай 2019 года из практики рентгенологического отделения ГБУЗ МО «Дубненская городская больница». В январе в кирпичном доме

на участке садоводческого товарищества был обнаружен труп мужчины. Обстановка на месте позволяла заподозрить взрывную травму – имелись характерные разрушения кирпичной кладки вокруг отопительного котла с разлётом кирпичей и цементной кладки, наличие копоти на окружающих предметах и теле. Учитывая большое внимание средств массовой информации, было принято решение провести компьютерную томографию посмертно. При исследовании сканов компьютерной томографии были замечены переломы костей черепа в зоне ран со смещением центральных отломков лобной, теменной костей, передней стенки левого верхнечелюстного синуса; отмечено большое количество газов в полости черепа и в ликворных пространствах головного мозга. Инородных частиц не обнаружено.

При последующем судебно-медицинском исследовании трупа было установлено, что основные повреждения располагались на голове: в виде ран, повреждений черепа и головного мозга – а также, поверхностные, на конечностях, не прикрытых одеждой. В зоне ран на голове отмечено наличие копоти, крошек кирпича, цементной кладки – признаки воздействия факторов взрыва.

В данном случае виртопсия сыграла роль предсекционного (предварительного) метода исследования тела, позволила установить и задокументировать

⁸ Mahesh Sh., Kumar S. R. Critical Evaluation and Contribution of Virtopsy to Solved Crime //

Research Journal of Forensic Sciences. 2015. Vol. 3 (1). P. 1–9.

расположение и характер костных повреждений черепа, направление смещения отломков, наличие газов в полости черепа, спланировать последовательность и методы секционного исследования трупа. Оперативное проведение КТ-исследования, установившее отсутствие специфических поражающих элементов в трупе, позволило подтвердить предварительную версию следствия о бытовом взрыве парового котла. Информация о смещении костных отломков и головного мозга, отсутствия специфических инородных поражающих элементов послужила дополнительным аргументом в пользу того, что все повреждения причинены в единых условиях, вследствие поражающих факторов взрыва в виде взрывной волны и высокой температуры, вторичных поражающих элементов в виде кирпичей и цементной крошки. Изображения сканов КТ послужили наглядным иллюстративным приложением к заключению эксперта⁹

Данный метод является эффективным и имеет ряд преимуществ по сравнению с традиционным судебно-медицинским вскрытием:

1. Не требуется непосредственного физического вмешательства в ткани, что предотвращает ошибки, связанные со смещением тканевых структур.

2. Полученные изображения можно хранить длительное время и подвергать повторной оценке экспертов.

3. Обзор анатомических структур зачастую затрудняет исследование черепа, позвоночника, лицевого скелета и др., а с помощью современных технологий это не составит труда.

4. Виртопсия позволяет врачу-рентгенологу увидеть точное местоположение инородного материала.

5. Данный метод значительно экономит рабочее время специалиста, так как МРТ занимает около 30 минут, и исключает влияние отрицательного человеческого фактора в случае невнимательного и некачественного осмотра тела.

Ещё одной немаловажной причиной, доказывающей преимущества виртопсии является тот факт, что не все люди положительно относятся к реальному вскрытию. Восприятие человеком факта смерти разное. В основном возникают сложности в моральном или религиозном плане: для представителей многих религий и общин крайне важно сохранять тело покойного¹⁰.

Так, в Торе существует ряд положений, запрещающих надругаться над мёртвым телом, оставлять его не погребённым на ночь, использовать труп и получать какую-либо выгоду.

⁹ Жулин С. А., Велибеков Ю. З. Применение посмертной компьютерной томографии (виртуальной аутопсии) в случае смерти от взрывной травмы // Судебная медицина. 2019. Т. 5, № S1. С. 56.

¹⁰ Virtopsy – the concept of a centralized database in forensic medicine for analysis and comparison of radiological and autopsy data / E. Aghayev, L. Staub, R. Dirnhofer [et al.] // Journal of forensic and legal medicine. 2008. Vol. 15, № 3. P. 135–140.

Родственники и близкие люди стараются приложить максимальные усилия, чтобы похоронить умершего достойно, проявив необходимое уважение к нему, поэтому негативно воспринимают вскрытие. Изучение тела с помощью 3D-технологий помогло бы найти компромисс между медицинской организацией и родными погибшего в вопросах установления причины смерти, характера повреждений и пр.

Однако у виртопсии существуют и недостатки.

1. Так, одним из них является невозможность ввести специальное контрастное внутривенное вещество, в результате чего кровь не циркулирует, а это значительно осложняет проведение анализа повреждений внутренних органов и сосудов. Для России это является большим минусом, так как наиболее частой причиной скоропостижной смерти в Российской Федерации являются сердечно-сосудистые заболевания, артериальная гипертензия и её осложнения: инсульты, инфаркты, кардиомиопатии и тромбозы лёгочной артерии¹¹.

2. Наблюдается низкая эффективность в диагностике травм полых органов, желудочно-кишечного тракта, мочевыделительной системы и разрыва диафрагмы.

3. Отсутствует возможность классического описания органов и тканей, доступная при внутреннем

исследовании трупа: консистенции, выраженности анатомической структуры, цвета, кровенаполнения, массы, содержимого полых органов.

4. Не разработана методика определения критериев давности повреждений, выявленных при виртуальной аутопсии.

5. Существуют технические сложности при исследовании трупов с большой массой и значительно увеличенными в объёме гнилостными изменениями¹².

6. Правовая и нормативная база использования посмертной 3D-визуализации в судебно-медицинском вскрытии трупа в нашей стране находится только на стадии проработки.

7. В мире прослеживается довольно нестабильная экономическая обстановка, которая оказывает негативное влияние на финансовое состояние стран, городов, медицинских и экспертных учреждений. Аппараты КТ и МРТ очень дорогостоящие, поэтому не каждый морг может себе позволить такие затраты на покупку оборудования.

8. Пока отсутствует необходимая база знаний и опыта у специалистов, осуществляющих вскрытие для проведения его с помощью современных 3D-технологий. Чтобы повысить качество и эффективность проведения судебно-медицинского вскрытия тел,

¹¹ Судебная медицина и судебно-медицинская экспертиза: национальное руководство / под ред. Ю. И. Пиголкина. М.: ГЭОТАРМедиа, 2014. С. 664–679.

¹² Возможности посмертной визуализации в судебно-медицинской экспертизе трупа:

обзор и критический анализ литературы / Л. С. Коков, А. Ф. Кинле, В. Е. Сеницын, Б. А. Филимонов // Лучевая диагностика. Судебная медицина. 2015. №1. С. 1-28.

необходимо ввести в штат судебно-медицинских организаций профессиональных рентгенологов, ведь далеко не все эксперты подготовлены для подобных исследований с помощью КТ и МРТ.

Таким образом, в настоящее время виртуальная аутопсия не может заменить традиционное судебно-медицинское вскрытие трупа, так как отсутствует правовая база её применения, а также не все исследования можно сделать виртуально. Оптимальным вариантом видится использование данного метода исследования в качестве дополнения к основному вскрытию для

установления причины смерти, особенно в сложных ситуациях (например, в качестве скринингового исследования при скоропостижной смерти для решения вопроса о наличии скрытых механических повреждений). С каждым годом учёные и специалисты предлагают новые пути развития виртопсии, поэтому, рано или поздно, проблема использования виртуального вскрытия будет решена. В качестве дополнительного метода виртуальная аутопсия имеет право на существование и в настоящее время, но, чтобы заменить «золотой стандарт», необходимо ещё очень много работы.

Список литературы

1. Абрикосов А. И. Техника патологоанатомических вскрытий трупов М.: Медицина, 1948. 166 с.
2. Возможности посмертной визуализации в судебно-медицинской экспертизе трупа: обзор и критический анализ литературы / Л. С. Коков, А. Ф. Кинле, В. Е. Синицын, Б. А. Филимонов // Лучевая диагностика. Судебная медицина. 2015. №1. С. 1-28.
3. Дадабаев В. К. Законодательная основа производства судебно-медицинской экспертизы и возможности применения рентгеновского метода компьютерной томографии (СКТ) в исследовании трупа / В. К. Дадабаев, А. А. Стрелков // Библиотека криминалиста. 2014. № 6. С. 275–280.
4. Жулин С. А. Применение посмертной компьютерной томографии (виртуальной аутопсии) в случае смерти от взрывной травмы / С. А. Жулин, Ю. З. Велибеков // Судебная медицина. 2019. Т. 5, № S1. С. 56.
5. Новые диагностические признаки утопления по результатам виртуальной аутопсии / В. А. Клевно, Ю. В. Чумакова, М. А. Кислов [и др.] // Судебная медицина, 2020. Т. 6, № 3. С. 53–57.
6. Судебная медицина и судебно-медицинская экспертиза: национальное руководство / под ред. Ю. И. Пиголкина. М.: ГЭОТАРМедиа, 2014. 727 с.
7. Mahesh Sh. Critical Evaluation and Contribution of Virtopsy to Solved Crime / Sh. Mahesh, S. R. Kumar // Research Journal of Forensic Sciences. 2015. Vol. 3 (1). P. 1–9.
8. Thali M. The Virtopsy Approach. 3D optical and radiological scanning and reconstruction in forensic medicine / M. Thali, R. Dirnhofer, P. Vock // Boca Raton, Fl: CRC Press; London NW. 2009.

9. Virtopsy – the concept of a centralized database in forensic medicine for analysis and comparison of radiological and autopsy data / E. Aghayev, L. Staub, R. Dirnhofer [et al.] // Journal of forensic and legal medicine. 2008. Vol. 15, № 3. P. 135–140.

10. Virtopsy – the Swiss virtual autopsy approach / M. J. Thali, C. Jackowski, L. Oesterhelweg [et al.] // Legal Medicine (Tokyo). 2007. Vol. 9. P. 100–104.

11. Virtopsy, a new imaging horizon in forensic pathology: virtual autopsy by postmortem multislice computed tomography (MSCT) and magnetic resonance imaging (MRI) a feasibility study / M. J. Thali, K. Yen, W. Schweizer [et al.] // Journal of Forensic Science. 2003. Vol. 48. P. 386–403.

12. Virtopsy: minimally invasive, imaging guided virtual autopsy / R. Dirnhofer, C. Jackowski, P. Vock [et al.] // Radio Graphics. 2006. Vol. 26. P. 1305–1333.

Nelly V. Racheva

PhD (Law), Associate Professor of the Department of Criminalistics,
Ural State Law University named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
ekaterinburg@mail.ru

Yana M. Slepukhina

Student,
Ural State Law University named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
yana_slepukhina@mail.ru

**VIRTUAL AUTOPSY. PROSPECTS FOR APPLICATION
IN THE RUSSIAN FEDERATION**

Abstract: The article is devoted to the use of the method of virtual autopsy. A parallel is drawn between the development of virtopsy in Russia with the practice of application in foreign countries, experience and achievements in this area are considered. The positive and negative aspects of using this method, as well as the prospects for application in the Russian Federation, are analyzed.

Keywords: murder, corpse, autopsy, forensic examination, virtual autopsy, computed tomography, magnetic resonance imaging.

Юдин Егор Витальевич

Младший научный сотрудник, аспирант,
Санкт-Петербургский государственный университет
(г. Санкт-Петербург, Российская Федерация)
yudinegorv@gmail.com

**ПРАВО ПАЦИЕНТА НА ПОЛУЧЕНИЕ ИНФОРМАЦИИ О СОСТОЯНИИ
ЗДОРОВЬЯ ПРИ ИСПОЛЬЗОВАНИИ МЕДИЦИНСКИХ ГЕНЕТИЧЕСКИХ
ТЕХНОЛОГИЙ: ПЕРЕОСМЫСЛЕНИЕ СУЩЕСТВУЮЩЕГО
ПРАВОВОГО МЕХАНИЗМА***

Аннотация: В статье рассматриваются существующие правовые механизмы реализации пациентом права на получение информации о состоянии здоровья и конфиденциальность сведений, связанных с проведёнными в отношении него обследованиями с использованием медицинских генетических технологий. Автор заключает, что существующее регулирование не в полной мере отражает специфику возникающих в связи с использованием медицинских генетических технологий общественных отношений.

Ключевые слова: генетические технологии, социальная значимость, медицинская помощь, геномика, геномная медицина, социальный риск, правовой механизм.

Для цитирования:

Юдин Е. В. Право пациента на получение информации о состоянии здоровья при использовании медицинских генетических технологий: переосмысление существующего правового механизма // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 274–279.

Федеральной технической программой	научно- развития	генетических технологий на 2019–2027 годы ¹ (далее – Программа 2019 г. ²) в
---------------------------------------	---------------------	-------------------------------------------------------------------------------------------------------

* Настоящая работа подготовлена в рамках поддержанного РФФИ научного проекта № 20-311-90051.

¹ Постановление Правительства РФ от 22 апреля 2019 г. № 479 «Об утверждении Федеральной научно-технической программы развития генетических технологий на 2019 - 2027 годы» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_323164/ (дата обращения: 09.05.2022).

² Указом Президента РФ от 28 марта 2022 г. № 160 «О внесении изменений в Указ Президента Российской Федерации от 28 ноября 2018 г. № 680 «О развитии генетических технологий в Российской Федерации», в Положение о совете по реализации Федеральной научно-технической программы развития генетических технологий на 2019–2027 годы, в составы совета и президиума

качестве одного из приоритетных направлений научно-технологического развития Российской Федерации определён переход к персонализированной медицине. Концептуальный подход к данному феномену определён приказом Министерства здравоохранения РФ от 24 апреля 2018 г. № 186 (далее – Приказ Минздрава РФ № 186)³. Персонализированная медицина, согласно Приказу Минздрава № 186, в первую очередь связана с использованием медицинских генетических технологий для исследования генетических характеристик пациентов, выявления определённых генетических вариантов, связанных с потенциальной возможностью возникновения определённых заболеваний, и формирования таргетной терапии, индивидуальной для конкретного пациента.

Следовательно, персонализированная медицина тесно связана с генетическими технологиями, которые применяются в медицинской деятельности, – медицинскими генетическими технологиями (далее – МГТ).

Использование МГТ позволяет формировать в сфере охраны здоровья граждан как систему, включающей совокупность политических, экономических, правовых, научных, медицинских, в т. ч. санитарно-противоэпидемических (профилактических) мер, новые социальные практики, трансформирующие существующую и по большей части патерналистскую модель организации здравоохранения и способствующие формированию пациент-ориентированного подхода, который характеризуется активным включением самого пациента в процесс оказания ему медицинской помощи, в данной сфере общественных отношений.

Медицинская деятельность является социально значимой⁴. Создание условий (в т. ч. и правовых) для оказания качественной и безопасной медицинской помощи является общественным обязательством государства, поименованным в Конституции РФ социальным, по обеспечению прав граждан на охрану здоровья и медицинскую помощь (статьи 7, 41 Конституции России)⁵. Указанное

совета, утвержденные этим Указом» с 28 марта 2022 г. период действия Программы 2019 г. был продлён до 2030 г.

³ Приказ Министерства здравоохранения РФ от 24 апреля 2018 г. № 186 «Об утверждении Концепции предиктивной, превентивной и персонализированной медицины» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_356205/ (дата обращения: 09.05.2022).

⁴ Определение Конституционного Суда РФ от 28 сентября 2021 г. № 1953-О «Об отказе в принятии к рассмотрению жалобы

гражданина Хохлова Василия Викторовича на нарушение его конституционных прав пунктом 3 части 1 статьи 100 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» // СПС «КонсультантПлюс».

URL: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=686459#6gNxn5TYIouGBVf5> (дата обращения: 09.05.2022)

⁵ Конституция Российской Федерации (принята на всенародном голосовании 12 декабря 1993 г.) (с изменениями, одобренными в ходе общероссийского

приобретает особое значение при использовании МГТ, т. к., обладая особой спецификой, они преобразуют саму медицинскую деятельность, наделяя её новыми особенностями, влияющими в т. ч. и на правовое регулирование возникающих общественных отношений.

Указанный объективный процесс активного внедрения МГТ не может не сказаться на автономии пациента как ключевом биоэтическом принципе, который в законодательстве об охране здоровья граждан нашёл своё правовое воплощение в виде норм, определяющих правовой статус пациента. В отношении же прав пациента, являющихся составной частью его правового статуса, действующее законодательство предусматривает специальные правовые механизмы их реализации, включающие в себя ряд правовых средств, которые определённым, наиболее оптимальным образом, организованы и направлены на упорядочивание общественных отношений в рассматриваемой сфере и на удовлетворение интересов субъектов права⁶.

Одним из правовых воплощений автономии пациента в действующем законодательстве об охране здоровья является право пациента на получение информации о состоянии своего здоровья, правовой механизм реализации которого закреплён в ст. 22 Федерального закона от 21 ноября 2011

г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» (далее – Закон № 323-ФЗ)⁷.

В первую очередь, п. 1 ст. 22 Закона № 323-ФЗ определяет содержательное наполнение понятия информации о состоянии здоровья. К ней относятся сведения, отражающие:

- результаты медицинского обследования;
- наличие заболевания;
- установленный диагноз;
- прогноз развития заболевания;
- методы оказания медицинской помощи;
- информацию о рисках использования тех или иных методов оказания медицинской помощи;
- возможные виды медицинского вмешательства;
- последствия осуществлённого медицинского вмешательства;
- результаты оказания медицинской помощи.

Далее раскрывается механизм реализации данного права, включающий в себя возможность получения пациентом такой информации лично от лечащего врача либо от других медицинских работников, которые непосредственно участвовали в медицинском обследовании и лечении (п. 2 ст. 22 Закона № 323-ФЗ).

голосования 1 июля 2020 г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 09.05.2022)

⁶ В данном случае – пациента и медицинского работника.

⁷ Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_121895/ (дата обращения: 09.05.2022).

Воплощая в нормах права автономию пациента, законодатель также закрепил очень важное нормативное положение, в соответствии с которым недопустимо сообщать информацию о состоянии здоровья против воли самого пациента (п. 3 ст. 22 Закона № 323-ФЗ). Здесь же содержится норма, наделяющая пациента возможностью запретить сообщать информацию о неблагоприятном прогнозе развития заболевания супругу (супруге), близким родственникам (дети, родители, усыновлённые, усыновители, родные братья и родные сестры, внуки, дедушки, бабушки).

Закреплённое в Конституции России (статьи 23, 24) право на неприкосновенность частной жизни, личную и семейную тайну реализуется, среди прочего, посредством сформированных законодателем правовых механизмов, устанавливающих специальные правовые режимы (в т. ч. режима ограничения свободного доступа) в отношении той или иной информации о частной жизни лица.

В сфере медицинского права в таком статусе выступает институт врачебной тайны, соблюдение которой является одним из принципов охраны здоровья (ст. 4 Закона № 323-ФЗ), а правовой механизм реализации данного принципа отражён в ст. 13 Закона № 323-ФЗ. Так, к врачебной тайне относятся сведения:

- об обращении гражданина за оказанием медицинской помощи;

- характеризующие состояние его здоровья;

- раскрывающие его диагноз;
- иные, полученные при его медицинском обследовании и лечении.

Статья 73 Закона № 323-ФЗ закрепила среди обязанностей медицинских работников требование соблюдать врачебную тайну. Разглашение таких сведений без согласия пациента не допускается (п. 3 ст. 13 Закона № 323-ФЗ), за исключением особых случаев.

Между тем, при использовании МГТ существующие правовые механизмы не могут в полной мере эффективно урегулировать возникшие правоотношения и обеспечить соблюдение прав и интересов (неправовой фактор, формирующий правовые средства⁸) всех заинтересованных субъектов данных отношений.

При использовании МГТ (например, при проведении молекулярно-генетического тестирования) медицинским работником формируются определённые сведения (генетическая информация) о пациенте. Медицинскому работнику необходимо проанализировать, интерпретировать данную информацию и сообщить пациенту о её клинической значимости для развития определённого заболевания, подтверждения диагноза и т. д.

Общественные отношения, складывающиеся в связи с

⁸ Дивеева Н. И. Функции индивидуального правового регулирования трудовых отношений // Вестник Томского

государственного университета. 2008. № 3. С. 123–126.

использованием МГТ, как ранее мы отмечали, характеризуются рядом особенностей, к числу которых относится особый порядок их регулирования. Такое регулирование строится на тесном переплетении как правовых, так и неправовых инструментов социального управления общественными отношениями. В связи с тем, что медицинская генетика находится в состоянии постоянного накопления новых знаний о связях генетических маркеров с различными заболеваниями и периодической переоценки уже имеющихся данных, то существенным компонентом в регулировании выступает само медицинское сообщество генетиков, реализующее свои полномочия посредством саморегулирования в рамках соответствующего медицинского сообщества.

Таким ярким примером являются изданные в 2015 г. Американским колледжем медицинской генетики и геномики (ACMG) и Ассоциацией молекулярной патологии рекомендации по классификации выявленных у пациентов генетических вариантов⁹, которые могут быть следующих видов:

- 1) Патогенный: более 99 % уверенности, что обнаруженный вариант вызовет заболевание;
- 2) Вероятно патогенный: более 90 % уверенности, что обнаруженный вариант вызовет заболевание;
- 3) Неизвестной значимости: 10–90 % уверенности, что обнаруженный вариант вызовет заболевание;

4) Вероятно доброкачественный: более 90 % уверенности, что обнаруженный вариант не вызовет заболевание;

5) Доброкачественный: более 99 % уверенности, что обнаруженный вариант не вызовет заболевание.

Как видно из представленной классификации, вероятность по многим обнаруженным генетическим вариантам, что они вызовут заболевание крайне неоднозначна. Более того, в процессе молекулярно-генетического тестирования может обнаружиться, что у данного пациента имеется генетический вариант, вызывающий определённое заболевание, но он находится в неактивной форме. Однако есть высокая доля вероятности, что такой же вариант имеется у его родственников (родителей, бабушек, дедушек и др.), и у кого-то из них он может быть активным.

Однако в рамках существующих правовых механизмов, направленных на обеспечение прав пациентов, медицинский работник может полагаться только на благоразумность самого пациента, что не всегда может быть оправданным, т. к. это создаёт угрозу причинения вреда здоровью или даже жизни другим лицам (неопределённому кругу лиц). Благополучие общества, учитывая действующие нормы зависит полностью от добросовестности пациента, что не может быть нами положительно оценено, т. к. первостепенной задачей в рассматриваемой сфере общественных

⁹ Opportunities, resources, and techniques for implementing genomics in clinical care / T. A.

Manolio, R. Rowley, M. S. Williams [et al.] // Lancet. 2019. Vol. 394. P. 511–520.

отношений является выстраивание правовых механизмов, которые соблюдали бы баланс частных и публичных интересов, учитывая

особую социальную значимость медицинской деятельности, особенно той, в которой используются генетические технологии.

Список литературы

1. Дивеева Н. И. Функции индивидуального правового регулирования трудовых отношений // Вестник Томского государственного университета. 2008. № 3. С. 123–126.
2. Opportunities, resources, and techniques for implementing genomics in clinical care / T. A. Manolio, R. Rowley, M. S. Williams [et al.] // Lancet. 2019. Vol. 394. P. 511–520.

Yegor V. Yudin

Junior research assistant, postgraduate student,
St. Petersburg State University
(Saint Petersburg, Russian Federation)
yudinegorv@gmail.com

THE PATIENT'S RIGHT TO RECEIVE INFORMATION ABOUT THE STATE OF HEALTH WHEN USING MEDICAL GENETIC TECHNOLOGIES: RETHINKING THE EXISTING LEGAL MECHANISM

Abstract: The article examines the existing legal mechanisms for the realization by the patient of the right to receive information about the state of health and confidentiality of information related to the examinations conducted in relation to him using medical genetic technologies. The author concludes that the existing regulation does not fully reflect the specifics of social relations arising in connection with the use of medical genetic technologies.

Keywords: genetic technologies, social significance, medical care, genomics, genomic medicine, social risk, legal mechanism.

УДК 347.1

Артамонова Дарья Алексеевна

Студент,

Уральский государственный юридический университет

имени В. Ф. Яковлева

(г. Екатеринбург, Российская Федерация)

dasha-artamonowa2018@yandex.ru

Научный руководитель – В. О. Пучков,

кандидат юридических наук, ассистент кафедры гражданского права

ПРАВОВАЯ ПРИРОДА ДОГОВОРА СУРРОГАТНОГО МАТЕРИНСТВА

Аннотация: В настоящее время активно развивается система вспомогательных репродуктивных технологий, что приводит к проблематике регулирования правоотношений, возникающих при их применении. Рассуждения о правовой природе договора суррогатного материнства и по сей день является достаточно дискуссионным вопросом. Подробнее разобраться в специфике данного договора мы попытаемся в нашем исследовании.

Ключевые слова: суррогатное материнство, договор, правовое регулирование, законодательство, соглашение.

Для цитирования:

Артамонова Д. А. Правовая природа договора суррогатного материнства // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 280–286.

По данным статистики, ежегодно с 2010 года количество циклов суррогатного материнства в Российской Федерации (далее – РФ) растёт на 250–400 единиц в год¹. Следовательно, возрастает популярность использования данного метода вспомогательных репродуктивных технологий (далее – ВРТ), что приводит к появлению новых проблем в правовом регулировании данного процесса, а

также возникновению морально-этических споров о восприятии столь неестественного процесса появления ребёнка на свет.

Суррогатное материнство охватывает перечень методик, общим признаком которых является то, что женщина вынашивает ребёнка для другого лица либо разно- или однополый пары. Эмбрион может быть зачат в лабораторных условиях с

¹ Статистика использования ВРТ // Росстат. URL: <https://rosstat.gov.ru/> (дата обращения: 30.03.2022).

использованием половых клеток пары, либо донорских материалов.

Споры о правовой природе договора, который заключается между родителями – «заказчиками» – и суррогатной матерью, являются серьёзной дискуссионной проблемой как во всём обществе, так и в юридическом мире. Является ли осуществление процесса вынашивания ребенка суррогатной матерью услугой? Влечёт ли за собой данная процедура использование тела женщины в качестве инструмента с целью получения материальной выгоды? Достаточно ли урегулирован данный вопрос на территории РФ и за рубежом?

Рассмотрим более подробно специфику регулирования суррогатного материнства в РФ. В настоящее время не существует специализированных актов, которые регулировали бы данную сферу всеобъемлюще, однако существует ряд документов, прямо или косвенно затрагивающих вопросы осуществления интересующего нас метода ВРТ. Так базовым актом в данной сфере является ФЗ «Об основах охраны здоровья граждан в РФ»², в пункте 9 ст. 55 которого закрепляется нормативная дефиниция суррогатного материнства как вынашивания и рождения ребёнка (в том числе преждевременные роды) по договору, заключаемому между суррогатной матерью (женщиной, вынашивающей

плод после переноса донорского эмбриона) и потенциальными родителями, чьи половые клетки использовались для оплодотворения, либо одинокой женщиной, для которых вынашивание и рождение ребёнка невозможно по медицинским показаниям. Стоит учесть, что к потенциальной суррогатной матери предъявляются особые требования, закрепленные в п. 10 той же статьи, например: возрастной ценз, наличие минимум одного здорового собственного ребёнка, соответствие критериев здоровья. В случае замужества потенциальной суррогатной матери для её участия в проекте экстракорпорального оплодотворения (далее – ЭКО) требуется письменное согласие супруга. Институт обязательного согласия супруга может рассматриваться как некое ограничение права женщины на распоряжение своим собственным телом³.

Процесс записи родителей ребёнка, рождённого с использованием суррогатного материнства, регулируется нормами Семейного кодекса РФ (далее – СК РФ). Запись родителей ребёнка в книге записей рождения отличается от классического процесса, который осуществляется после естественного появления на свет. В случае рождения ребёнка суррогатной матерью необходимо её разрешение для документального

² Федеральный закон от 21.11.2011 № 323-ФЗ (ред. от 26.03.2022) «Об основах охраны здоровья граждан в Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_121895/ (дата обращения: 10.05.2022).

³ Майфат А. В., Лисаченко А. В. Тело человека, его отдельные части как объекты правового воздействия (некоторые предложения для обсуждения) // Юридический мир. 2002. № 2. С.10.

закрепления биологических родителей в актах рождения. Аналогичная норма нашла своё отражение и в Федеральном законе «Об актах гражданского состояния»⁴. Данное расширение прав суррогатной матери может привести к злоупотреблению правом. Конституционный суд РФ, разъяснил, что делать в случае возникновения такой проблемы. Если суррогатная мать отказалась дать согласие на запись родителями доноров биологического материала, учитывая все фактические обстоятельства конкретного дела, в том числе связанные с тем, заключался ли договор о суррогатном материнстве и каковы его условия, являются ли истцы генетическими родителями ребёнка, по каким причинам суррогатная мать не дала согласия на запись истцов в качестве родителей ребёнка, и руководствуясь положениями статьи 3 Конвенции о правах ребенка (далее – КПР)⁵, разрешить спор в интересах ребёнка.

Исходя из определения суррогатного материнства, вынашивание и рождение ребенка осуществляется после заключения договора. Каким же образом он может регулироваться?

Для начала обратимся к общепринятому пониманию договора в российском законодательстве. Так, согласно 420 статье Гражданского

кодекса РФ (далее – ГК РФ), под договором понимается соглашение двух или нескольких лиц об установлении, изменении или прекращении гражданских прав и обязанностей. Также, по общему правилу, к договорам применяются правила о двух- многосторонних сделках⁶. Процесс осуществления вынашивания плода суррогатной матерью невозможно признать коммерческой сделкой либо актом оказания возмездной услуги по статье 779 ГК РФ, несмотря на то, что такая процедура зачастую предусматривает денежное вознаграждение, ведь в данном случае денежные средства рассматриваются как компенсация за претерпевание самого процесса беременности и родов, который может протекать для женщины с осложнениями. Также стоит отметить, что оплата медицинских услуг, питания и иных расходов, которые необходимы для здорового и безопасного течения беременности суррогатной матери, биологическими родителями не может быть признаком возмездности в данном случае, так как данные расходы являются необходимыми издержками для появления на свет здорового ребенка. Денежное или же иное возмещение может расцениваться как благодарность биологических родителей за оказанную суррогатной

⁴ Федеральный закон от 15.11.1997 № 143-ФЗ (ред. от 30.12.2021) «Об актах гражданского состояния» // СПС «КонсультантПлюс». URL:

http://www.consultant.ru/document/cons_doc_LAW_16758/ (дата обращения: 10.05.2022).

⁵ Конвенция о правах ребенка (одобрена Генеральной Ассамблеей ООН 20.11.1989) //

СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_9959/ (дата обращения: 10.05.2022).

⁶ Гонгало Б. М. Гражданское право: учебник. В 2 т. / под ред. Б. М. Гонгало. Т. 1. М: Статут, 2016. С. 247.

матерью помощь. Придерживаясь этой позиции, мы можем признать идею использования тела суррогатной матери в качестве инструмента для достижения финансовой выгоды, в ходе вынашивания ребенка по программе суррогатного материнства, крайне несостоятельной, так как признак возмездности проявляется не явно и в данном случае практически неизмерим с усилиями, которые были приложены суррогатной матерью. Выплату денежной компенсации по субъективному характеру можно сравнить с моральным вредом, так как проявление морального вреда включает в себя следующие категории: внутренний дискомфорт, переживания, страх, ощущение незащищённости, порой беспомощности, боязни за свои жизнь и здоровье, уязвимость. Что с психологической точки зрения может частично описать моральное состояние суррогатной матери, которая находится в определённом психологическом напряжении, вынашивая не своего ребенка.

Так, по мнению Е. А. Батлера, если договор не является гражданско-правовым, то в случае неисполнения или ненадлежащего исполнения сторонами его условий невозможно применять нормы гражданско-правовой ответственности⁷. И в этом случае вознаграждение суррогатной матери выходит за рамки правового поля. С другой стороны, если рассматривать договор как гражданско-правовой, то возникает

вопрос о его правовой принадлежности в рамках гражданского права.

А. А. Пестрикова придерживается мнения, что при заключении договора между супругами и суррогатной матерью предмет договора – вынашивание ребёнка, т. е. оказание своеобразной услуги, за которую суррогатная мать получает вознаграждение. Супруги обязуются оказывать материальную помощь суррогатной матери в период её беременности, включая оплату всех медицинских расходов, отсутствие забот у суррогатной матери и т. д. Суррогатная мать, в свою очередь, обязуется соблюдать условия договора, предусматривающие обязательное прохождение медицинских осмотров, соблюдение установленного режима, выполнение всех предписаний выбранного супругами врача и прочее, а самое главное – передачу ребёнка, после его рождения, супругам⁸. Исходя из данной концепции, в случае неисполнения договора суррогатная мать по ст. 782 ГК РФ обязана будет возместить все затраты, которые были понесены генетическими родителями – «заказчиками».

Договор суррогатного материнства также отличается и от договора подряда. В нём речь идёт об обязанности подрядчика выполнить по заданию заказчика определённую работу. Однако действия суррогатной матери нельзя назвать работой в том смысле, в котором понимает это слово

⁷ Батлер Е. А. Непоименованные договоры: некоторые вопросы теории и практики: автореф. дис. ... канд. юрид. наук. М., 2006. С. 16.

⁸ Пестрикова А. А. Проблемы договора о суррогатном материнстве. М., 2006. С. 6.

законодатель. Работа всегда гарантирует результат. В отношениях суррогатного материнства гарантировать результат невозможно. Об отличии договора суррогатного материнства от договора подряда свидетельствует и то обстоятельство, что в договоре подряда подрядчик вправе привлечь к исполнению своих обязанностей других лиц (субподрядчиков), если из закона или договора не следует обязанность подрядчика выполнить предусмотренную в договоре работу лично, а по договору о суррогатном материнстве суррогатная мать обязана оказать услуги лично.

Передачу ребёнка суррогатной матерью, даже в случае признания гражданско-правового характера данного договора, нельзя признать предметом договора, а ребёнка – предметом сделки, так как это бы противоречило нормам нравственности и правопорядка. Ведь после отделения от организма матери посредством родов плод считается полноправным субъектом права, к нему применяется термин ребёнок⁹, что в данном случае отождествляется с временным этапом развития человека. В случае признания ребёнка предметом сделки нарушался бы установленный запрет на торговлю людьми.

Таким образом, невозможно применять к договору суррогатного материнства исключительно

существующие положения ГК РФ, регулирующие имущественные отношения, так как у данных соглашений существует множество особенностей, которые по этическим причинам не могут быть урегулированы только данными нормами. Невозможно представить также, чтобы суррогатная мать, вынашивая и рожая ребёнка, оказывала услуги либо же выполняет некоторую работу. Ведь услуги и работы, как объекты гражданского права, имеют известную имущественную ценность. В случае реализации договора о суррогатном материнстве невозможно оценить материальную ценность рождённого ребёнка или помощь суррогатной матери парам, которые не могут зачать ребенка самостоятельно, никакими экономическими благами, несмотря на то, что СК РФ не закрепляет императивного запрета на возмездное исполнение данной процедуры. Приравнивание договора суррогатного материнства к договорам возмездного оказания услуг видится невозможным, так как суррогатная мать может оказывать помощь как на возмездной, так и на безвозмездной основе¹⁰.

Анализ существующих норм гражданского законодательства наталкивает на мысль о необходимости выделения отдельного вида договора, а именно договора о суррогатном материнстве.

⁹ Федеральный закон от 21.11.2011 № 323-ФЗ (ред. от 26.03.2022) «Об основах охраны здоровья граждан в Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_121895/ (дата обращения: 10.05.2022).

¹⁰ Журавлёва С. П. Место договора о суррогатном материнстве среди других гражданско-правовых договоров // Современное право. 2011. № 4. С. 64–66.

Проанализировав нормативный массив РФ, представляем возможным сделать вывод о необходимости совершенствования правового регулирования института суррогатного материнства. Отношения, касающиеся новейших медицинских технологий, в том числе репродуктивных, часто развиваются намного быстрее, чем законодательство, регулирующее их. Вопрос о регулировании суррогатного материнства, по нашему мнению, не должен сводиться к классической модели регулирования имущественных отношений, так как в ходе вынашивания и рождения ребёнка суррогатной матерью помимо имущественных, появляется определённый перечень личных неимущественных отношений, которые также дополнительно регулируются СК РФ, как в отношении суррогатной матери, так и родителей – «заказчиков».

Споры в научной среде и социуме долгое время не могут принести желаемых результатов, так как регулирование суррогатного материнства касается не только «сухой» буквы закона, но и принципов этики, норм морали. Данные вопросы сложны для регулирования, ведь

каждый индивид трактует их через призму собственного опыта и взглядов на жизнь.

Наиболее перспективным является создание исключительного правового режима для договора суррогатного материнства, который бы учитывал право женщины на распоряжение своим телом и его возможностями, но также закреплял ещё большее количество гарантий для биологических родителей, которые помогли бы избежать утраты ими возможности воспитывать своего ребёнка, в случаях противоречия законодательства стран проживания суррогатной матери и родителей – «заказчиков» либо разногласия между сторонами договора. А также введение в ГК РФ самостоятельной нормы, регулирующей договор суррогатного материнства.

Совершенствование правового регулирования этого вопроса сыграет огромную роль в развитии репродуктивных прав человека, а также поможет закрепить и сформировать более гуманное и этичное отношение людей в обществе к суррогатному материнству и детям, которые были рождены с использованием данной технологии.

Список литературы

1. Батлер Е. А. Непоименованные договоры: некоторые вопросы теории и практики: автореф. дис. ... канд. юрид. наук. М., 2006. 28 с.
2. Гонгало Б. М. Гражданское право: учебник. В 2 Т. / под ред. Б. М. Гонгало. Т. 1. М: Статут, 2016. 511 с.
3. Журавлева С. П. Место договора о суррогатном материнстве среди других гражданско-правовых договоров // Современное право. 2011. № 4. С. 64–66.

4. Майфат А. В. Тело человека, его отдельные части как объекты правового воздействия (некоторые предложения для обсуждения) / А. В. Майфат, А. В. Лисаченко // Юридический мир. 2002. № 2. С. 4–15.

5. Пестрикова А. А. Проблемы договора о суррогатном материнстве // Гражданское право. М.: Юрист, 2006. № 2. С. 14–17.

Daria A. Artamonova

Student,

Ural State Law University
named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
dasha-artamonowa2018@yandex.ru

Scientific supervisor – V. O. Puchkov, PhD (Law),
Assistant of the Department of Civil Law

THE LEGAL NATURE OF THE SURROGACY CONTRACT

Abstract: Currently, the system of assisted reproductive technologies is actively developing, which leads to the problems of regulating legal relations arising from their application. Reasoning about the legal nature of the surrogacy contract is still quite a debatable issue. We will try to understand the specifics of this agreement in more detail in our research.

Keywords: surrogacy, contract, legal regulation, legislation, agreement.

УДК 34.01

Кушнарёв Александр Сергеевич

Студент,

Уральский государственный юридический университет

имени В. Ф. Яковлева

(г. Екатеринбург, Российская Федерация)

kushnarev-02@list.ru

Научный руководитель – И. Ю. Крылатова, кандидат юридических наук, доцент кафедры конституционного права, директор Центра биоэтики и права Уральского государственного юридического университета имени В. Ф. Яковлева

О НЕКОТОРЫХ ПРОБЛЕМАХ ПРАВОВОГО РЕГУЛИРОВАНИЯ ТЕХНОЛОГИИ МНОГОМЕРНОЙ БИОПЕЧАТИ

Аннотация: Как известно, современные аддитивные технологии (3D-биопринтинг) являются действенным средством спасения жизни и восстановления граждан. Однако стремительное развитие новых медицинских методов детерминирует необходимость решения сложнейших биоэтических проблем, связанных с обеспечением уважения человеческого достоинства и недопущения нарушения целостности индивида. В связи с чем в данной работе рассматриваются возможные риски внедрения трёхмерной биопечати в отечественную трансплантологию, а также представлены возможные варианты их решения.

Ключевые слова: биоэтика, 3D-биопринтинг, трансплантология, биоэтические риски.

Для цитирования:

Кушнарёв А. С. О некоторых проблемах правового регулирования технологии многомерной биопечати // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 287–292.

В настоящее время, по самым скромным подсчётам, в трансплантации органов нуждается примерно 200 тысяч человек по всему миру. Согласно данным Американского департамента здоровья и медицинской помощи, 21 человек в день умирает, не дождавшись пересадки. В российские «листы ожидания» каждый год записывается примерно по 5 тысяч человек. Однако

только у 10 % больных есть шанс дожждаться трансплантации.

Если учесть развитие современных медицинских технологий и рост продолжительности жизни, становится очевидным, что потребность в донорских органах будет расти, равно как и их нехватка – увеличиваться, а развитие трёхмерной биопечати даст потенциальным реципиентам шанс на получение

сконструированного биологического трансплантата, который способен частично или полностью восстановить утраченную функцию. В связи с этим необходимо провести комплексный анализ претворения в нормативное поле такого явления как трёхмерный биопринтинг, чтобы выявить определённые биоэтические риски использования трёхмерной биопечати в отечественной трансплантологии. Без адекватного доктринального ответа на новейшие технологические вызовы современности невозможно представить, как минимум, последующее выстраивание нормативно-правой среды, формирование применимых правовых режимов и институтов.

Особую зону рисков использования биопринтинга составляют вопросы защиты информации и персональных данных. Сама по себе технология 3D биопринтинга предполагает на первом этапе воспроизведение в цифровой форме модели будущего органа (CAD-файл), которая в последующем будет использована для его печати. В данном случае можно говорить о персонализированном характере самой цифровой модели, т. е. цифрового образа, обращённого к конкретному человеку, что в свою очередь фактически приводит к стиранию границ между физическим миром и цифровым пространством. И, как отмечал Д. Е. Богданов, так называемая «диджитализация» тела человека ставит под угрозу сущность самой природы человека как уникального биологического существа. Представляется возможным, что массивы человеческой

информации, содержащиеся на CAD-файлах, могут стать реальными объектами хищения со стороны злоумышленников – потенциальные правонарушители смогут незаконно продавать цифровые модели органов человека неограниченному числу лиц, что безусловно будет являться нарушением личных неимущественных прав владельцев CAD-файлов.

В контексте рассматриваемой выше возможности использования продуктов биопринтинга, на мой взгляд, возникает очевидный пример столкновения публичных и частных интересов. Так, например, при возможном закреплении законодателем презумпции всеобщего согласия на последующее использование CAD-файлов открывается ряд перспективных возможностей, прежде всего в научной сфере – дальнейшее распространение цифровых моделей может ускорить развитие изучения отдельных человеческих патологий, предоставит новые возможности и для развития систем поддержки принятия врачебных решений. Однако при этом обязательно должны соблюдаться требования добровольности и полной информированности владельца цифрового образа, согласие не должно взиматься в случае, если обладатель цифровой модели находится в заведомо уязвимом положении. Подобная точка зрения была высказана и в Постановлении ЕСПЧ по делу «Коновалова против Российской Федерации», где Европейский Суд недвусмысленно указал, что согласие пациента считается добровольным, если на пациента не оказывалось

давление или ненадлежащее влияние. Более того, на сферу использования биопринтинговых органов представляется возможным распространить признанный международным сообществом принцип приоритета интересов личности над интересами общества, отражение которого можно увидеть в ст. 10 Всеобщей декларации о геноме человека и правах человека: никакое научное исследование, касающееся природы человеческого организма, не должно превалировать над уважением прав человека, его основных свобод и человеческого достоинства.

Наиболее рациональным решением подобной ситуации, на мой взгляд, является принятие отдельного самостоятельного законодательного акта, который сможет устранить выявленные выше пробелы правового регулирования, а также вывести продукты биопринтинга из-под действия «смежных» правовых актов, что в последующем позволит избежать все возможные правовые риски.

Особого внимания заслуживает рассмотрение биоэтических рисков, возникающих при использовании технологии трёхмерной биопечати, ведь где как ни в технологии биопринтинга мы можем наблюдать очевидный конфликт во взаимоотношениях между биомедицинскими знаниями и технологиями, с одной стороны, и человеком как биологическим существом – с другой.

И главный вопрос, который является извечным в сфере отечественной трансплантологии, а также применим к сфере биопринтинга – возможно ли коммерциализировать

продукты биопринтинга? Либо же к таковым продуктам должны по аналогии с обращением человеческих органов применяться нормы отечественного законодательства, запрещающие любые коммерческие действия, предметом которых будут выступать биопринтинговые органы? Так, согласно ст. 1 Закона РФ «О трансплантации органов и (или) тканей человека» № 4180–1 запрещается осуществление сделок купли-продажи, предметом которых будут выступать органы или ткани человека. Однако, как мы установили в начале нашего исследования, биопринтинговые органы во многом отличны от органов человека, в связи с чем не представляется возможным распространение вышеупомянутой нормы и на отношения, связанные с коммодификацией продуктов биопринтинга. Означает ли это очередной пробел в правовом регулировании? На мой взгляд, возможности коммерциализации биопринтинговых органов и тканей может привести к усилению социальной стратификации, условному господству богатых над бедными, где последние будут вынуждены отказываться от жизни «биологической» ради достойного поддержания жизни «социальной». Истоками введения запрета на осуществление коммерческих действий, предметом которых будут выступать человеческие органы и ткани, являются победившая в начале XX века идеология о человеке как высшей ценности и Стамбульская декларация о трансплантационном туризме и торговле органами, закрепившие принцип финансового

нейтралитета. Более того, запрет на извлечение финансовой выгоды закреплён в статье 21 Конвенции о защите прав и достоинства человека в связи с применением достижений биологии и медицины, он также тесно связан с понятием человеческого достоинства и признан практически во всём мире. В таком случае законодатель при регулировании вопросов коммодификации биопринтинговых органов обязательно должен формировать национальную «биополитику» с учётом общепризнанных концепций равенства прав и свобод человека и гражданина, а также верховенства человеческой жизни.

Другой проблемой в рамках нашего биоэтического дискурса выступает этичность использования клеток эмбрионов при производстве «биочернил». Как известно, эмбриональные стволовые клетки обладают предрасположенностью к неограниченному размножению и способны дифференцироваться практически в любые типы клеток, в связи с чем являются идеальным материалом для печати будущих органов и тканей. Однако, по сути, происходит уничтожение человеческих эмбрионов ради получения как раз-таки эмбриональных стволовых клеток, которые в последующем будут использованы для производства органов и тканей. В западной литературе высказывалось мнение, что эмбрион *in vitro*, из которого получают в дальнейшем необходимые клетки, имеет тот же этический статус, что и человек и, соответственно, он в такой же степени достоин защиты. Так, в

постановлении по делу «Парилло против Италии», вынесенном в 2015 г., Европейский Суд установил, что «защиту жизненного потенциала эмбриона можно связать с целью охраны нравственности и защиты прав и свобод других лиц», что может оправдывать запрет на использование человеческих эмбрионов для производства биочернил, направленных на спасение других жизней, ибо их уничтожение можно считать самым настоящим преступлением.

На данный момент российское законодательство, регулирующее вопросы биопринтных органов и тканей, содержит в себе множество спорных моментов, влекущих за собой как правовые, так и биоэтические риски. Подобное положение дел актуализирует необходимость скорейшего определения модели правового регулирования технологии биопечати.

Представляется, что наиболее верным решением вопроса по урегулированию правоотношений в сфере биопринтных объектов и технологии биопринтинга является принятие отдельного самостоятельного акта, который будет направлен на определение модели правового регулирования аналогичной законодательству о трансплантации органов и тканей. По аналогии с Законом РФ № 4180–1 возможным наименованием закона видится – «О трёхмерной биопечати органов и (или) тканей человека». В рамках данного законодательного акта предметом будут выступать общественные отношения, складывающиеся по поводу производства, обращения,

распространения и имплантации биопринтинговых органов и тканей. Представляется необходимым определить круг субъектов обращения и распространения CAD-файлов для защиты личных неимущественных прав их владельцев, а также самих продуктов биопечати; установление базовых дефиниций технологии биопечати; закрепление принципов осуществления деятельности в сфере обращения продуктов биопринтинга, среди которых по аналогии с Федеральным законом «О биомедицинских клеточных продуктах» обязательно должен быть указан принцип «недопустимости создания эмбриона человека в целях производства биопринтингового материала», что позволит решить этическую проблему создания биочернил. Более того, новый

законодательный акт должен будет вывести объекты биопринтинга из-под действия «смежных» правовых актов, например, всё того же Федерального закона о биомедицинских клеточных продуктах, что позволит избежать образовавшиеся правовые коллизии.

Безусловно, создание законодательного акта, регулирующего продукты биопринтинга и его технологию, не сможет полностью решить все потенциальные правовые проблемы, однако подобный шаг позволит в определенной степени нивелировать все те правовые и биоэтические риски, которые были рассмотрены выше, и что самое главное – устранил текущее состояние правовой неопределённости в регулировании биопринтных органов и тканей.

Alexander S. Kushnarev
Student,
Ural State Law University
named after V.F. Yakovlev
(Yekaterinburg, Russian Federation)
kushnarev-02@list.ru

Scientific supervisor – I. Yu. Krylatova, PhD (Law), Associate Professor of the Department of Constitutional Law, Director of the Center for Bioethics and Law of the Ural State Law University named after V.F. Yakovlev

ON SOME PROBLEMS OF LEGAL REGULATION TECHNOLOGIES OF MULTIDIMENSIONAL BIOPRINTING

Abstract: Modern additive technologies (3D bioprinting) are known to be an effective means to save lives and restore citizens. However, the rapid development of new medical techniques determines the need to address the complex bioethical issues associated with the need to ensure respect for human dignity and avoid violating the integrity of the individual. For this reason, this paper examines the possible risks of introducing three-dimensional bioprinting into domestic transplantology and presents

possible solutions.

Keywords: bioethics, 3D bioprinting, transplantation, bioethical risks.

Научное издание

ТЕХНОЛОГИИ XXI ВЕКА В ЮРИСПРУДЕНЦИИ

Материалы
Четвёртой международной научно-практической конференции

(г. Екатеринбург, 20 мая 2022 года)

*Материалы публикуются в авторской редакции, авторы несут
ответственность за оригинальность и научно-теоретический уровень
публикуемого материала.*

Компьютерная вёрстка: Д. В. Бахтеев

Корректоры: К. В. Бахтеева, А. Д. Цветкова

Рисунок на обложке: Андрей tramdrey Негруль

**Уральский государственный юридический университет
имени В. Ф. Яковлева**

620137, г. Екатеринбург, ул. Комсомольская, 21
usla.ru

АНО «КримЛиб»

Основной сайт: hub.crimlib.info

Энциклопедия: Crimlib.info

Канал: t.me/crimlib

ae@crimlib.info

Союз криминалистов и криминологов

crimescience.ru

Электронное издание